BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

IDENTIFICATION SYSTEM

Patent number: JP2002297551

Publication date: 2002-10-11

Inventor: OKUDA HARUHISA; HIRAI TAKAHIDE; SHIKAI MASAHIRO; SHIROTSUKI AKIHIDE; OKA TORU; TATSUBO HIROKAZU; TSUTADA HIROYUKI

Applicant: MITSUBISHI ELECTRIC CORP

Classification:

- international: G06F15/00; G06K17/00; G06K19/00; H04L9/32

- european:

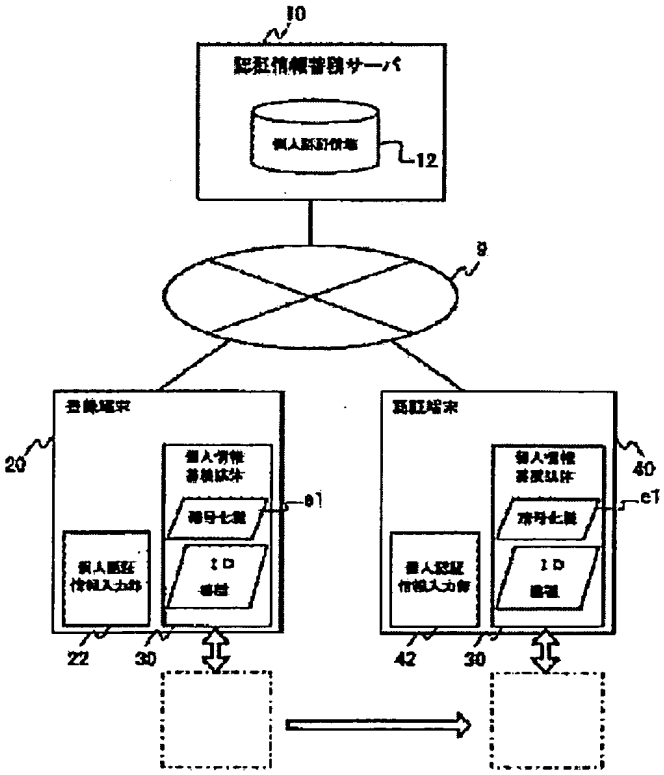
Application number: JP20010101906 20010330

Priority number(s):

Abstract of **JP2002297551**

PROBLEM TO BE SOLVED: To obtain an identification system which safely and surely performs user identification even between different terminals.

SOLUTION: Biometrics information such as fingerprints, irises and handwriting of a user is encoded by using a registration terminal 20 beforehand and registered in an identification information storage server 10. Also, key information for use in encoding and decoding it, registration terminal model information and user identification information are recorded in a portable personal information storage medium 30. When receiving identification in an identification terminal 40, encoded biometrics information acquired from the above identification information storage server 10 is decoded by using the encoding key e1 of the personal information storage medium 30. The user identification is performed by collating the decoded biometrics information with the reentered biometrics information.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－297551
（P2002－297551A）
(43)公開日　平成14年10月11日(2002.10.11)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)	
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｆ	５Ｂ０３５
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｖ	５Ｂ０５８
	19/00			19/00	Ｑ	５Ｂ０８５
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ	５Ｊ１０４
					６７５Ａ	

審査請求　未請求　請求項の数５　ＯＬ　（全 21 頁）　最終頁に続く

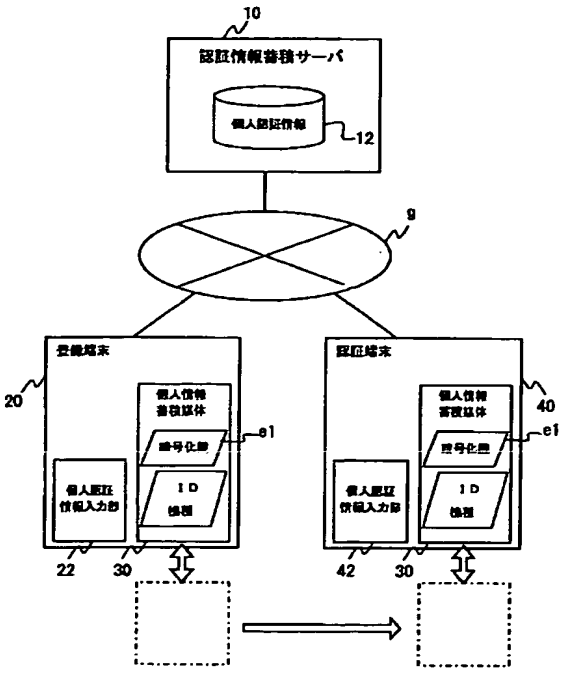
(21)出願番号　特願2001－101906(P2001－101906)
(22)出願日　平成13年３月30日(2001.3.30)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　奥田　晴久
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　平井　敬秀
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　認証システム

(57)【要約】
【課題】　ユーザ認証を、異なる端末間においても安全かつ確実におこなう認証システムを得ること。
【解決手段】　あらかじめ登録端末２０を用いてユーザの指紋、虹彩、筆跡等のバイオメトリクス情報を暗号化して認証情報蓄積サーバ１０に登録するとともにその暗号化および復号化のための鍵情報、登録端末機種情報、ユーザＩＤ情報を搬送可能な個人情報蓄積媒体３０に記録しておき、認証端末４０において認証を受ける際に、上記した認証情報蓄積サーバ１０から取得した暗号済みのバイオメトリクス情報をその個人情報蓄積媒体３０の暗号化鍵ｅ１を用いて復号し、復号化したバイオメトリクス情報と、改めて入力したバイオメトリクス情報とを照合することでユーザの認証をおこなう。



1

【特許請求の範囲】
【請求項１】　少なくとも暗号化鍵を記録した個人情報蓄積媒体と、
ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、
を備え、
前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする認証システム。
【請求項２】　少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、
ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、
電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、
を備え、
前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする認証システム。
【請求項３】　少なくとも暗号化鍵を記録した個人情報蓄積媒体と、
ユーザの第１のバイオメトリクス情報を入力し、入力した第１のバイオメトリクス情報を複数の第２のバイオメトリクス情報に分割し、各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第２のバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの第２のバイオメトリクス情報を蓄積し、蓄積した第２のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第２のバイオメトリクス情報を併合して前記第１のバイオメトリクス情報を復元し、復元した第１のバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、
を備え、
前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする認証システム。
【請求項４】　少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、
ユーザの第１のバイオメトリクス情報を入力し、入力した第１のバイオメトリクス情報を複数の第２のバイオメトリクス情報に分割し、各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第２のバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの第２のバイオメトリクス情報を蓄積し、蓄積した第２のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第２のバイオメトリクス情報を併合して前記第１の

バイオメトリクス情報を復元し、復元した第１のバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、

電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、

を備え、

前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする認証システム。

【請求項５】　前記認証情報蓄積サーバが蓄積したバイオメトリクス情報と同内容のバイオメトリクス情報を蓄積した複数のミラーサーバを備え、

前記登録端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つに対して、前記暗号化したバイオメトリクス情報を送信し、

前記認証端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つから、前記暗号化したバイオメトリクス情報を受信することを特徴とする請求項１～４のいずれか一つに記載の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信回線を介してサービスを享受する際のユーザ認証をおこなう認証システムに関し、特に、そのユーザ認証を、異なる端末間においても安全かつ確実におこなうことができる認証システムに関するものである。

【０００２】

【従来の技術】近年において急速に広まったインターネットは、オープンなネットワークであるがゆえに、自分が送信したデータが第三者に盗み見される可能性を否定できないという問題を有している。そこで、暗号化技術を導入することで、ＷｅｂサーバとＷｅｂブラウザとの間でクレジット・カード番号などを安全に送信したり、メールの送信者や内容が偽造されたりしていないことを証明するといったデータの保安性が図られている。

【０００３】ここで、インターネット上の暗号化技術の代表的なものとしては、共通鍵暗号法と公開鍵暗号法が知られている。共通鍵暗号法は、自分と相手が同じ暗号鍵を使って暗号化と復号化をおこなう方法である。一

方、公開鍵暗号法は、現在主流となっている暗号方法であり、秘密鍵と公開鍵という二つの鍵ペアを用いて暗号化と復号化をおこない、どちらか一方の鍵で暗号化したデータは、もう一方の鍵を使わないと復号化できないという特徴を有している。

【０００４】この公開鍵暗号法において、秘密鍵は、その名の通り、所持者（使用権限のある者）だけが自由に使うことができるため、自身で安全に管理しなければいけない。また、公開鍵は、インターネット上等で広く公開されており、誰でも取得して利用できるようにされている。ここで、秘密鍵を使って暗号化することは、復号化するための公開鍵を誰もが入手できるので一見意味がない様に思えるが、実はそうではなく、秘密鍵を使ってデータを暗号化すれば、そのデータをペアとなる公開鍵で復号化することにより、確かにそのデータが秘密鍵保持者によって暗号化されたことを確認できるという利点を有している。すなわち、これにより本人性を確認することができ、この性質を利用したものが、いわゆるデジタル署名である。

【０００５】デジタル署名は、送信者（作成者）を特定するために、電子的に作成された文書（メッセージ）に添付され、電子商取引や電子申請をサポートする電子認証システムにおいて、非常に重要な役割を果たしている。具体的には、送信者により作成されたメッセージからハッシュ値を抽出することでメッセージの縮小版であるメッセージダイジェストを作成し、つづいてこのメッセージダイジェストを送信者自身の秘密鍵で暗号化することにより作成される。

【０００６】デジタル署名を利用した認証システムは、認証書保持者（メッセージ送信者）、認証書依拠者（メッセージ受信者）および認証局（公開鍵認証書発行者）の三者により構成されるのが一般的である。ここで、公開鍵認証書とは、メッセージ送信者が誰であるかを確認できるものであり、通常、認証を受けたメッセージ送信者の公開鍵とそのメッセージ送信者に関する情報（属性）とが含まれている。また、公開鍵認証書は認証局から発行され、発行を受けた本人のみが、その認証書に対応する秘密鍵を使用することができる。さらに、公開鍵認証書には、発行元の認証局を明らかにするために、認証局のデジタル署名がされている。よって、認証局は、強い公共性を持った場合が多い。

【０００７】一方、ユーザ認証をおこなう方法の一つして、バイオメトリクス認証が注目されている。バイオメトリクス認証とは、指紋、虹彩、掌紋、音声、筆跡などの個人に固有の生体情報に基づいて、ユーザを特定する方法である。よって、バイオメトリクス情報の入力に際しては、本人以外がそれを実行することは不可能であり、より安全性の高いユーザ認証が可能となる。

【０００８】このようなバイオメトリクス情報をユーザ認証に利用した認証システムとしては、例えば特開２０

００－０９２０４６号に「遠隔認証システム」が開示されている。この「遠隔認証システム」によれば、ユーザの個人情報であるバイオメトリクス情報を暗号化し、バイオメトリクス情報をユーザが指定した認証サーバにのみ復号可能な状態でネットワークを転送するので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できる。

【０００９】

【発明が解決しようとする課題】しかしながら、上記したデジタル署名によるユーザ認証では、一度、コンピュータ等の利用端末にデジタル署名を登録した後は、ユーザ認証時においてパスワードの入力が必要になるのみで、他人にパスワードが知られた場合に、その利用端末からのなりすましを防ぐことはできなかった。すなわち、ユーザ本人とデジタル署名との関連付けは、認証局等からデジタル署名を取得する際に必要となるだけであり、パスワードの漏洩といったソーシャルハッキングに対抗できるものではなかった。

【００１０】一方、上記した特開２０００－０９２０４６号に開示の「遠隔認証システム」では、認証サーバ側でバイオメトリクス情報を復号できため、サーバ側で悪意を持ったオペレーションがおこなわれた場合、情報を完全に保護することができないという問題があった。

【００１１】また、照合対象となるバイオメトリクス情報、すなわち登録されたバイオメトリクス情報を、携帯可能な記録媒体に記録することも可能であるが、一般にバイオメトリクス情報のサイズは、デジタル署名等に比較して非常に大きく、大容量の記録媒体を必要とするため、現実的ではない。さらに、その記録媒体が盗難にあった場合には、バイオメトリクス情報を解析して、なりすましも可能となる可能性が高い。

【００１２】この発明は上記問題点を解決するためになされたもので、ユーザ認証を、異なる端末間においても安全かつ確実におこなう認証システムを得ることを目的とする。

【００１３】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、この発明にかかる認証システムにあっては、少なくとも暗号化鍵を記録した個人情報蓄積媒体と、ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人

情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、を備え、前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする。

【００１４】この発明によれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバが管理するので、認証端末のように、ユーザが登録時に使用した登録端末とは異なる端末を利用しようとする場合でも、個人情報蓄積媒体を移すことのみで、暗号化をともなった個人認証を実行することが可能となる。

【００１５】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、を備え、前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする。

【００１６】この発明によれば、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、アプリケーションサーバ側が要求するユーザ認証を可能にする。

【００１７】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵を記録した個人情報蓄積媒体

と、ユーザの第１のバイオメトリクス情報を入力し、入力した第１のバイオメトリクス情報を複数の第２のバイオメトリクス情報に分割し、各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第２のバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの第２のバイオメトリクス情報を蓄積し、蓄積した第２のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第２のバイオメトリクス情報を併合して前記第１のバイオメトリクス情報を復元し、復元した第１のバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、を備え、前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする。

【００１８】この発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなる。

【００１９】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、ユーザの第１のバイオメトリクス情報を入力し、入力した第１のバイオメトリクス情報を複数の第２のバイオメトリクス情報に分割し、各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第２のバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの第２のバイオメトリクス情報を蓄積し、蓄積した第２のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第２のバイオメトリクス情報を受信し、受信した暗号化済みの各第２のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第２のバイオメトリクス情報を併合して前記第１のバイオメトリクス情報を復元し、復元した第１のバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、を備え、前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする。

【００２０】この発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するとともに、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、また、アプリケーションサーバ側が要求するユーザ認証を可能にする。

【００２１】つぎの発明にかかる認証システムにあっては、上記発明において、前記認証情報蓄積サーバが蓄積したバイオメトリクス情報と同内容のバイオメトリクス情報を蓄積した複数のミラーサーバを備え、前記登録端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つに対して、前記暗号化したバイオメトリクス情報を送信し、前記認証端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つから、前記暗号化したバイオメトリクス情報を受信することを特徴とする。

【００２２】この発明によれば、複数の認証情報蓄積サーバにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができる。

【００２３】

【発明の実施の形態】以下に、この発明にかかる認証システムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【００２４】実施の形態１．まず、実施の形態１にかかる認証システムについて説明する。実施の形態１にかかる認証システムは、あらかじめ登録端末を用いてユーザの指紋、虹彩、筆跡等のバイオメトリクス情報を暗号化して認証情報蓄積サーバに登録するとともにその暗号化および復号化のための鍵情報、登録端末機種情報、ユーザＩＤ情報を搬送可能な個人情報蓄積媒体に記録しておき、認証端末において認証を受ける際に、上記した認証情報蓄積サーバから取得した暗号済みのバイオメトリク

ス情報をその個人情報蓄積媒体の暗号化鍵を用いて復号し、復号化したバイオメトリクス情報と、改めて入力したバイオメトリクス情報とを照合することでユーザの認証をおこなうことを特徴としている。

【００２５】図１は、実施の形態１にかかる認証システムの概略構成を示すブロック図である。図１において、実施の形態１にかかる認証システムは、認証情報蓄積サーバ１０と、登録端末２０と、認証端末４０とを備えて構成され、これらは通信回線９を介して通信可能に接続されている。

【００２６】認証情報蓄積サーバ１０は、インターネット上のＷｅｂサーバと同様な構成であり、いわゆる一般的なコンピュータシステムである。但し、ここで、認証情報蓄積サーバ１０は、登録端末２０から送信された個人認証情報を登録して蓄積するとともに、認証端末４０からの要求に応じて、蓄積された個人認証情報を返信する。

【００２７】登録端末２０は、通信回線９を介して提供される電子商取引等の種々のサービスを享受することができるデスクトップコンピュータ、ノートコンピュータ、ＰＤＡ（Personal Digital Assistant）、携帯電話等と同様な装置構成に、バイオメトリクス情報を入力することが可能な個人認証情報入力部２２と、個人情報蓄積媒体３０とを設けて構成される。

【００２８】認証端末４０は、登録端末２０の個人認証情報入力部２２と同構成の個人認証情報入力部４２と、個人情報蓄積媒体３０とを設けて構成され、全体の構成は登録端末２０と変わりない。よって、登録端末２０と認証端末４０とは装置構成上特に区別されないが、少なくとも双方において、個人認証情報入力部２２および４２と個人情報蓄積媒体３０を装填可能なスロットとはそれぞれ共通の仕様である必要がある。

【００２９】例えば、個人認証情報入力部２２および４２は、バイオメトリクス情報としてユーザの指紋を入力する場合には、指紋スキャナであり、バイオメトリクス情報としてユーザの筆跡を入力する場合にはスタイラスペンを用いて入力可能なタブレットのような入力パッドである。

【００３０】また、個人情報蓄積媒体３０は、携帯が容易な不揮発性記憶媒体であり、例えば、磁気カード、フラッシュメモリカード、ＩＣカードなどである。よって、登録端末２０には、この個人情報蓄積媒体３０を装填することが可能なスロットが設けられている。

【００３１】また、通信回線９は、有線か無線かを問わず、公衆の電話回線網でも専用回線であってもよい。また、それら通信回線上に構築されたインターネット等のＩＰ網をも含む。

【００３２】以下に、実施の形態１にかかる認証システムの動作について説明する。図２は、実施の形態１にかかる認証システムの動作を示すフローチャートである。図２において、まず、ユーザは、登録端末２０の個人認証情報入力部２２を介して、その個人認証情報入力部２２において入力可能な自己のバイオメトリクス情報を入力する（ステップＳ１０１）。例えば、個人認証情報入力部２２が指紋スキャナである場合には、登録端末２０は、指紋スキャナで読み取った指紋画像から特徴点照合法に基づく特徴点を抽出し、抽出した特徴点の情報をバイオメトリクス情報として取得する。

【００３３】つぎに、登録端末２０は、取得したバイオメトリクス情報に対して、所定の暗号化鍵ｅ１により暗号処理を施す（ステップＳ１０２）。なお、この暗号化鍵ｅ１は、ユーザＩＤ情報や登録端末２０の機種情報等とともに、個人情報蓄積媒体３０に記録されている。

【００３４】つづいて、登録端末２０は、暗号化されたバイオメトリクス情報を、上記したユーザＩＤ情報や登録端末２０の機種情報等とともに、通信回線９を介して認証情報蓄積サーバ１０に送信する（ステップＳ１０３）。認証情報蓄積サーバ１０は、暗号化済みのバイオメトリクス情報等の登録情報を受け取ると、個人認証情報データベース１２に、その登録情報を登録する（ステップＳ２０１）。

【００３５】ユーザは、以上のような手順によってバイオメトリクス情報の登録処理を終えると、登録端末２０に装填していた個人情報蓄積媒体３０を取り外し、認証端末４０において認証処理が必要な場合以外は携帯等により厳重に保管しておく。特に、個人情報蓄積媒体３０は、利用制限された建造物の入退出時や電子マネーの利用時などの他の認証をおこなうＩＤカードとしての機能を兼用させてもよく、この場合、ユーザは、複数の記録媒体を携帯する必要がなく、利用時の混乱も生じなくなる。

【００３６】つぎに、ユーザは、登録端末２０とは異なる認証端末４０を使用する際、その認証端末４０に個人情報蓄積媒体３０を装填する。そして、ユーザは、認証端末４０自体を使用する際に、または、認証端末４０によって通信回線９を介したサービスを享受する際に要求されるユーザ認証に対して、登録端末２０を用いたバイオメトリクス情報の入力手順と同様に、認証端末４０の個人認証情報入力部４２を介して、自己のバイオメトリクス情報を入力する（ステップＳ３０１）。

【００３７】認証端末４０は、ユーザによって入力されたバイオメトリクス情報を一端保持し、認証情報蓄積サーバ１０に向けて、登録済みの個人認証情報、すなわち暗号化済みのバイオメトリクス情報の要求を、個人情報蓄積媒体３０に記録されたユーザＩＤ情報や登録端末２０の機種情報等とともに発信する（ステップＳ３０２）。

【００３８】認証情報蓄積サーバ１０は、認証端末４０から上記個人認証情報要求を受け取ると、その個人認証情報要求に含まれるユーザＩＤ情報や登録端末２０の機

種情報等に応じた暗号済みのバイオメトリクス情報を、個人認証情報データベース１２から取り出し、認証端末４０に返信する（ステップＳ２０２）。

【００３９】認証端末４０は、認証情報蓄積サーバ１０から暗号済みのバイオメトリクス情報を受け取ると、その暗号済みのバイオメトリクス情報を、個人情報蓄積媒体３０に記録された暗号化鍵ｅ１を用いて復号化する（ステップＳ３０３）。そして、認証端末４０は、この復号化で得られたバイオメトリクス情報と、上記ステップＳ３０１において入力されたバイオメトリクス情報とを照合し、両者が一致しているかを判断する（ステップＳ３０４）。

【００４０】認証端末４０は、両者が一致していると判断すると、認証端末４０自体の使用や通信回線９を介したサービスの享受が可能な状態に移行し、その旨のメッセージ等を表示する。逆に、両者が一致していない場合には、バイオメトリクス情報の再入力を促すメッセージや警告等を表示する。

【００４１】以上に説明したとおり、実施の形態１にかかる認証システムによれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバ１０が管理するので、登録端末２０と認証端末４０のように、ユーザが登録時とは異なる端末を利用しようとする場合でも容易に個人認証を実行することが可能となる。

【００４２】また、異なる端末間において利用可能な個人情報蓄積媒体３０に暗号化鍵ｅ１を記録しているので、その暗号化鍵ｅ１で暗号化されたバイオメトリクス情報を、個人情報蓄積媒体３０を介して復号化することができ、結果的に、認証情報蓄積サーバ１０上に、バイオメトリクス情報を暗号化した状態で蓄積しておくことができる。換言すると、個人情報蓄積媒体３０を装填していない端末では、ユーザ認証が不可能であり、高い安全性が確保される。

【００４３】また、上記個人情報蓄積媒体３０には少なくとも暗号／復号のための鍵情報のみを保持すればよいので、バイオメトリクス情報のサイズが大きい場合でも、個人情報蓄積媒体３０の記憶量を圧迫することはない。例えば、バイオメトリクス情報が指紋情報の場合、複数の認証端末間において異なる指紋スキャナが備えられている場合であっても、登録端末２０の指紋スキャナと認証端末４０の指紋スキャナの仕様が一致さえしていれば、ユーザ一人に対して、複数の異なる仕様の指紋スキャナごとの指紋情報を登録することで、それぞれ個人認証が可能となる。

【００４４】また、これは、ユーザ一人に対して、同じ種類のバイオメトリクス情報だけでなく異なる種類のバイオメトリクス情報を登録して利用できることを意味する。例えば、認証情報蓄積サーバ１０に、一人のユーザに対して、指紋情報と筆跡情報の双方を暗号化した状態で登録し、指紋スキャナを備えた認証端末と入力パッドを備えた認証端末の双方においてユーザ認証をおこなうことが可能である。すなわち、登録端末の機種情報を用いることで複数の異なる認証用機構を使い分けることができる。

【００４５】実施の形態２．つぎに、実施の形態２にかかる認証システムについて説明する。実施の形態２にかかる認証システムは、電子商取引サービスの提供等をおこなうアプリケーションサーバからユーザ認証が求められた場合に、アプリケーションサーバによって公開鍵で暗号化されたセッションキーを受け取り、秘密鍵で復号化してそのセッションキーを取り出すとともに、取り出したセッションキーと実施の形態１にかかる認証システムによって照合された照合結果とをさらに秘密鍵で暗号化してアプリケーションサーバに返送することで、アプリケーションサーバにおいてより信頼性の高いユーザ認証を可能としたことを特徴としている。

【００４６】図３は、実施の形態２にかかる認証システムの概略構成を示すブロック図である。なお、図３において、図１と共通する部分には同一の符号を付してその説明を省略する。図３に示す認証システムでは、登録端末２０および認証端末４０に装填される個人情報蓄積媒体３０に、暗号化鍵ｅ１に加えて、秘密鍵Ｅｓ１の情報が記録されている点と、アプリケーションサーバ５０を備えている点が、図１と異なる。

【００４７】ここで、アプリケーションサーバ５０は、通信回線９と接続されて電子商取引等の種々のサービスを提供するとともに、上記秘密鍵Ｅｓ１と対になる公開鍵を入手しており、ユーザ認証の手順として、認証端末４０に対するセッションキーＫｓ１の発行をおこなう。なお、具体的な装置構成は、認証情報蓄積サーバ１０と同様のコンピュータシステムである。

【００４８】以下に、実施の形態２にかかる認証システムの動作について説明する。図４は、実施の形態２にかかる認証システムの動作を示すフローチャートである。なお、実施の形態２にかかる認証システムの動作において、図２に示したステップＳ１０１～Ｓ１０３、Ｓ２０１、Ｓ２０２、Ｓ３０１～Ｓ３０４の各処理は共通するため、ここでは特にそれらの説明を省略する。特に、図４では、説明を簡単にするため、図２に示したステップＳ１０１～Ｓ１０３、Ｓ２０１の図示を省略している。

【００４９】よって、ここでは、認証端末４０による照合処理（ステップＳ３０４）の後の動作について説明する。認証端末４０における照合処理が終わった後、ユーザが、アプリケーションサーバ５０が提供するサービスを享受したいとして、そのアプリケーションサーバ５０にアクセスしたとすると、アプリケーションサーバ５０は、このアクセスに対して、まず、セッションキーを乱数生成する。つづいて、アプリケーションサーバ５０は、生成したセッションキーを、あらかじめ入手してい

た公開鍵Ｅｐ１で暗号化した後（ステップＳ４０１）、認証端末４０に向けて送信する（ステップＳ４０２）。ここで、アプリケーションサーバ５０が入手している公開鍵Ｅｐ１は、そのアプリケーションサーバ５０によるサービスを利用しようとしているユーザ固有の鍵であり、そのユーザが保持している秘密鍵Ｅｓ１と対になるものである。

【００５０】アプリケーションサーバ５０による公開鍵Ｅｐ１の入手は、例えば、ユーザが初めてそのアプリケーションサーバ５０にアクセスした際に、アプリケーションサーバ５０からユーザに対して公開鍵Ｅｐ１を送信する旨の指示を与えることによって実現される。なお、ユーザは、そのユーザ固有の公開鍵Ｅｐ１および秘密鍵Ｅｓ１の鍵ペアを、第三者信用機関である認証局から取得してもよいし、認証情報蓄積サーバ１０が発行することにより取得してもよく、特に限定しない。

【００５１】認証端末４０は、アプリケーションサーバ５０から暗号済みのセッションキーを受け取ると、個人情報蓄積媒体３０に記録された秘密鍵Ｅｓ１を用いてセッションキーを復号化する（ステップＳ３０５）。さらに、認証端末４０は、ステップＳ３０４においておこなわれた照合の結果を示すメッセージとステップＳ３０５において復号化されたセッションキーとを秘密鍵Ｅｓ１を用いて暗号化し（ステップＳ３０６）、アプリケーションサーバ５０に送信する（ステップＳ３０７）。

【００５２】アプリケーションサーバ５０は、認証端末４０から、暗号化された照合結果およびセッションキーを受け取ると、公開鍵Ｅｐ１を用いて復号化し、復号化された照合結果が一致を示し、かつ復号されたセッションキーがステップＳ４０２において認証端末４０に送信したものと一致しているか否かを照合する（ステップＳ４０３）。一致している場合には、正当なユーザからのアクセスであると判断され、アプリケーションサーバ５０は、上記セッションキーまたは新たに発行したセッションキーと、秘密鍵および公開鍵とを用いた、いわゆる共通鍵暗号法と公開鍵暗号法とを組み合わせた暗号通信により、サービスの提供をおこなう。

【００５３】このように、アプリケーションサーバ５０が認証端末４０に対してサービスを提供する際には、通常、そのセキュリティを向上させるためにセッションキーの発行をおこなっており、本実施の形態では、そのセッションキーを、ユーザ認証をおこなうために利用している。

【００５４】以上に説明したとおり、実施の形態２にかかる認証システムによれば、実施の形態１にかかる認証システムの構成に対して、個人情報蓄積媒体３０にさらに秘密鍵Ｅｓ１の情報を記録し、アプリケーションサーバ５０が発行するセッションキーと認証端末４０上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りすることで、アプリケーションサーバ５０側が要求するユーザ認証をも可能にするので、実施の形態１による効果に加え、アプリケーションサーバ５０側から見て、信頼度の高いユーザ認証をおこなうことができる。

【００５５】実施の形態３．つぎに、実施の形態３にかかる認証システムについて説明する。実施の形態３にかかる認証システムは、実施の形態１において示した認証情報蓄積サーバを複数設置し、なおかつ各認証情報蓄積サーバは同内容の個人認証情報データベースを備えていることを特徴としている。

【００５６】図５は、実施の形態３にかかる認証システムの概略構成を示すブロック図である。なお、図５において、図１と共通する部分には同一の符号を付してその説明を省略する。図５に示す認証システムでは、複数の認証情報蓄積サーバ１０－１～１０－ｎを備えている点が、図１と異なる。

【００５７】特に、各認証情報蓄積サーバが備えている個人認証情報データベース１２は、同内容であり、登録端末２０および認証端末４０は、いずれの認証情報蓄積サーバに対しても、登録処理またはバイオメトリクス情報取得処理をおこなうことができる。

【００５８】例えば、登録端末２０が、認証情報蓄積サーバ１０－１に対し、実施の形態１において説明したようにバイオメトリクス情報の登録処理をおこなった場合には、認証情報蓄積サーバ１０－１は、個人認証情報データベース１２において登録処理により変更のあった部分を、他の認証情報蓄積サーバ１０－２～１０－ｎに通知し、認証情報蓄積サーバ１０－２～１０－ｎは、それぞれその通知に従って自己が備える個人認証情報データベース１２の内容を更新する。

【００５９】すなわち、認証情報蓄積サーバ１０－１～１０－ｎは、互いにミラーサーバの関係にあり、常に、同一の内容のバイオメトリクス情報を保持する。よって、認証端末４０は、いずれの認証情報蓄積サーバにアクセスしたとしても、最新のバイオメトリクス情報を取得することができる。なお、認証端末４０において、通信経路の最も短い位置にある認証情報蓄積サーバをあらかじめ登録しておき、通常利用時にはその認証情報蓄積サーバを利用するようにしてもよい。この際、その通常利用時の認証情報蓄積サーバが、何らかの障害によってダウンした場合には、自動的に、他の認証情報蓄積サーバに切り替わるように設定しておくことができる。

【００６０】以上に説明したとおり、実施の形態３にかかる認証システムによれば、複数の認証情報蓄積サーバ１０－１～１０－ｎにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となる。また、特に、応答速度の速い認証情報蓄積サーバを通常利用時のサーバに設定しておくことで、ネットワークトラフィックの状況によらず、迅速な認証

が可能となり、認証要求を出した端末と登録端末が地理的に異なる地点であっても、その影響を受けない認証が可能である。

【００６１】実施の形態４．つぎに、実施の形態４にかかる認証システムについて説明する。実施の形態４にかかる認証システムは、登録端末を用いて入力したバイオメトリクス情報を複数の情報に分割し、分割した各情報を暗号化して複数の認証情報蓄積サーバに分散して蓄積し、その暗号化および復号化のための鍵情報、登録端末機種情報、ユーザＩＤ情報、分散した認証情報蓄積サーバの情報を搬送可能な個人情報蓄積媒体に記録することを特徴としている。

【００６２】図６は、実施の形態４にかかる認証システムの概略構成を示すブロック図である。図６において、実施の形態４にかかる認証システムは、第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）と、登録端末１２０と、認証端末１４０とを備えて構成され、これらは通信回線９を介して通信可能に接続されている。

【００６３】第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）は、実施の形態１で説明した認証情報蓄積サーバ１０と同様な構成である。但し、第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）の各認証情報蓄積サーバにおいて蓄積されるバイオメトリクス情報は、互いに異なっている。

【００６４】登録端末１２０は、実施の形態１で説明した登録端末２０と同様な構成であり、個人認証情報入力部１２２と、個人情報蓄積媒体３０とを設けているが、それらに加えてさらに認証情報分割部１２４を備えている。認証情報分割部１２４は、個人認証情報入力部１２２を介して入力されたバイオメトリクス情報を複数の情報に分割する手段である。例えば、個人認証情報入力部１２２によって指紋画像が読み込まれたとすると、その指紋画像から特徴点照合法に基づく特徴点を抽出するとともに、抽出した特徴点の情報をさらに、端点や分岐点等の種類、位置、隆線間隔別の情報に分割する。

【００６５】認証端末１４０は、実施の形態１で説明した認証端末４０と同様な構成であり、個人認証情報入力部１４２と、個人情報蓄積媒体３０とを設けているが、それらに加えてさらに認証情報併合部１４４を備えている。認証情報併合部１４４は、登録端末１２０の認証情報分割部１２４によって分割されたバイオメトリクス情報を元の一つのバイオメトリクス情報に復元する手段である。

【００６６】また、個人情報蓄積媒体３０は、実施の形態１と同様に、携帯が容易な不揮発性記憶媒体であり、通信回線９は、実施の形態１と何ら変わりない。

【００６７】以下に、実施の形態４にかかる認証システムの動作について説明する。図７は、実施の形態４にかかる認証システムの動作を示すフローチャートである。図７において、まず、ユーザは、実施の形態１に説明したように、登録端末１２０の個人認証情報入力部１２２を介して、その個人認証情報入力部１２２において入力可能な自己のバイオメトリクス情報を入力する（ステップＳ１１１）。

【００６８】つぎに、登録端末１２０は、取得したバイオメトリクス情報に対し、認証情報分割部１２４によって、所定の複数のバイオメトリクス情報に分割する（ステップＳ１１２）。特に、第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）がそれぞれ蓄積する情報の種別に対応するように分割される。

【００６９】さらに、登録端末１２０は、複数に分割された各バイオメトリクス情報に対して、所定の暗号化鍵ｅ１により暗号処理を施す（ステップＳ１１３）。なお、この暗号化鍵ｅ１は、ユーザＩＤ情報や登録端末１２０の機種情報等とともに、個人情報蓄積媒体３０に記録されている。ここで、分割された各バイオメトリクス情報に対して用いる暗号化鍵ｅ１は、共通のものであってもよいし、各情報間で異なるものであってもよい。なお、この暗号化鍵ｅ１は、ユーザＩＤ情報、登録端末１２０の機種情報および登録先である第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）の各サーバ情報等とともに、個人情報蓄積媒体３０に記録されている。

【００７０】つづいて、登録端末１２０は、暗号化された各バイオメトリクス情報を、上記したユーザＩＤ情報や登録端末１２０の機種情報等とともに、通信回線９を介して、個人情報蓄積媒体３０に記録された上記サーバ情報に基づいて、第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）に送信する（ステップＳ１１４）。第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）の各サーバは、暗号化済みのバイオメトリクス情報等の登録情報を受け取ると、個人認証情報データベース１２に、その登録情報を登録する（ステップＳ２１１）。

【００７１】ユーザは、以上のような手順によってバイオメトリクス情報の登録処理を終えると、登録端末１２０に装填していた個人情報蓄積媒体３０を取り外し、実施の形態１において説明してように、認証端末１４０において認証処理が必要な場合以外は携帯等により厳重に保管しておく。

【００７２】つぎに、ユーザは、認証端末１４０を使用する際、その認証端末１４０に個人情報蓄積媒体３０を装填する。そして、ユーザは、認証端末１４０自体を使用する際に、または、認証端末１４０によって通信回線９を介したサービスを享受する際に要求されるユーザ認証に対して、登録端末１２０を用いたバイオメトリクス情報の入力手順と同様に、認証端末１４０の個人認証情

報入力部１４２を介して、自己のバイオメトリクス情報を入力する（ステップＳ３１１）。

【００７３】認証端末１４０は、ユーザによって入力されたバイオメトリクス情報を一端保持し、個人情報蓄積媒体３０に記録されたサーバ情報により決定される第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）に向けて、登録済みの個人認証情報、すなわち暗号化済みのバイオメトリクス情報の要求を、個人情報蓄積媒体３０に記録されたユーザＩＤ情報や登録端末１２０の機種情報等とともに発信する（ステップＳ３１２）。

【００７４】第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）の各サーバは、認証端末１４０から上記個人認証情報要求を受け取ると、その個人認証情報要求に含まれるユーザＩＤ情報や登録端末１２０の機種情報等に応じた暗号済みのバイオメトリクス情報を、個人認証情報データベース１２から取り出し、認証端末１４０に返信する（ステップＳ２１２）。

【００７５】認証端末１４０は、第１の認証情報蓄積サーバ１００（１）～第ｎの認証情報蓄積サーバ１００（ｎ）の各サーバから暗号済みのバイオメトリクス情報を受け取ると、各暗号済みのバイオメトリクス情報を、それぞれ個人情報蓄積媒体３０に記録された暗号化鍵ｅ１を用いて復号化する（ステップＳ３１３）。さらに、認証端末１４０は、この復号化で得られた各バイオメトリクス情報を、認証情報併合部１４４によって、元の一つのバイオメトリクス情報に併合して復元する（ステップＳ３１４）。

【００７６】そして、認証端末１４０は、この併合によって得られたバイオメトリクス情報と、上記ステップＳ３１１において入力されたバイオメトリクス情報とを照合し、両者が一致しているかを判断する（ステップＳ315）。

【００７７】認証端末１４０は、両者が一致していると判断すると、認証端末１４０自体の使用や通信回線９を介したサービスの享受が可能な状態に移行し、その旨のメッセージ等を表示する。逆に、両者が一致していない場合には、バイオメトリクス情報の再入力を促すメッセージや警告等を表示する。

【００７８】以上に説明したとおり、実施の形態４にかかる認証システムによれば、実施の形態１による効果を享受できるとともに、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなる。また、各認証情報蓄積サーバは分割されたバイオメトリクス情報を保持しているので、一つの認証情報蓄積サーバに蓄積されたバイオメトリクス情報のみではユーザ認証を受けることができず、高い安全性が確保される。

【００７９】また、端末間で移動する個人情報蓄積媒体３０には少なくとも分散先となる認証情報蓄積サーバと分割されたバイオメトリクス情報の種別とを含めたサーバ情報を保持すればよいので、バイオメトリクス情報のサイズが大きい場合でも、個人情報蓄積媒体３０の記憶量を圧迫することない。

【００８０】実施の形態５．つぎに、実施の形態５にかかる認証システムについて説明する。実施の形態５にかかる認証システムは、実施の形態２において示した認証情報蓄積サーバを、実施の形態３に示したように複数設置し、なおかつ各認証情報蓄積サーバは同内容の個人認証情報データベースを備えていることを特徴としている。

【００８１】図８は、実施の形態５にかかる認証システムの概略構成を示すブロック図である。なお、図８において、図３と共通する部分には同一の符号を付してその説明を省略する。図８に示す認証システムでは、図５に示したように、複数の認証情報蓄積サーバ１０－１～１０－ｎを備えている点が、図３と異なる。

【００８２】以上に説明したとおり、実施の形態５にかかる認証システムによれば、実施の形態２による効果を享受することができるとともに、複数の認証情報蓄積サーバ１０－１～１０－ｎにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となる。また、特に、応答速度の速い認証情報蓄積サーバを通常利用時のサーバに設定しておくことで、ネットワークトラフィックの状況によらず、迅速な認証が可能となり、認証要求を出した端末と登録端末が地理的に異なる地点であっても、その影響を受けない認証が可能である。

【００８３】実施の形態６．つぎに、実施の形態６にかかる認証システムについて説明する。実施の形態６にかかる認証システムは、実施の形態４において示した第１の認証情報蓄積サーバ～第ｎの認証情報蓄積サーバの各サーバを、さらに実施の形態３に示したように複数設置することを特徴としている。

【００８４】図９は、実施の形態６にかかる認証システムの概略構成を示すブロック図である。なお、図９において、図５および図６と共通する部分には同一の符号を付してその説明を省略する。図９に示す認証システムでは、第１の認証情報蓄積サーバ１０－１（１）～第ｍの認証情報蓄積サーバ１０－１（ｍ）の各サーバに対して、複数のミラーサーバを設置している点が、図６と異なる。例えば、第１の認証情報蓄積サーバ１０－１（１）に対しては、同一のバイオメトリクス情報を蓄積した複数の第１の認証情報蓄積サーバ１０－２（１）～１０－ｎ（１）が設置される。

【００８５】以上に説明したとおり、実施の形態６にか

かる認証システムによれば、実施の形態４にかかる認証システムにおいて、分割されたバイオメトリクス情報を分散して蓄積する第１の認証情報蓄積サーバ１０－１（１）～第ｍの認証情報蓄積サーバ１０－１（ｍ）の各サーバについて、実施の形態３において示したように複数のミラーサーバを設けるので、実施の形態４による効果に加え、実施の形態３による効果を享受することができる。

【００８６】なお、実施の形態６に示したように、分割されたバイオメトリクス情報を複数の認証情報蓄積サーバに分散させるとともに、各認証情報蓄積サーバに複数のミラーサーバを設置する構成は、実施の形態２にかかる認証システムに適用させることも可能であることは言うまでもない。

【００８７】

【発明の効果】以上、説明したとおり、この発明によれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバが管理するので、認証端末のように、ユーザが登録時に使用した登録端末とは異なる端末を利用しようとする場合でも、個人情報蓄積媒体を移すことのみで、暗号化をともなった個人認証を実行することが可能となるとともに、個人情報蓄積媒体を装填していない端末では、ユーザ認証が不可能となり、高い安全性が確保されるという効果を奏する。

【００８８】つぎの発明によれば、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、アプリケーションサーバ側が要求するユーザ認証を高い信頼度で可能にするという効果を奏する。

【００８９】つぎの発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、結果的に一つの認証情報蓄積サーバに蓄積されたバイオメトリクス情報のみではユーザ認証を受けることができず、高い安全性が確保されるという効果を奏する。

【００９０】つぎの発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するとともに、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、高い安全性を確保することができるとともに、アプリケーションサーバ側が要求するユーザ認証を高い信頼度で可能にするという効果を奏する。

【００９１】つぎの発明によれば、複数の認証情報蓄積サーバにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となるという効果を奏する。

【図面の簡単な説明】

【図１】　実施の形態１にかかる認証システムの概略構成を示すブロック図である。

【図２】　実施の形態１にかかる認証システムの動作を示すフローチャートである。

【図３】　実施の形態２にかかる認証システムの概略構成を示すブロック図である。

【図４】　実施の形態２にかかる認証システムの動作を示すフローチャートである。

【図５】　実施の形態３にかかる認証システムの概略構成を示すブロック図である。

【図６】　実施の形態４にかかる認証システムの概略構成を示すブロック図である。

【図７】　実施の形態４にかかる認証システムの動作を示すフローチャートである。

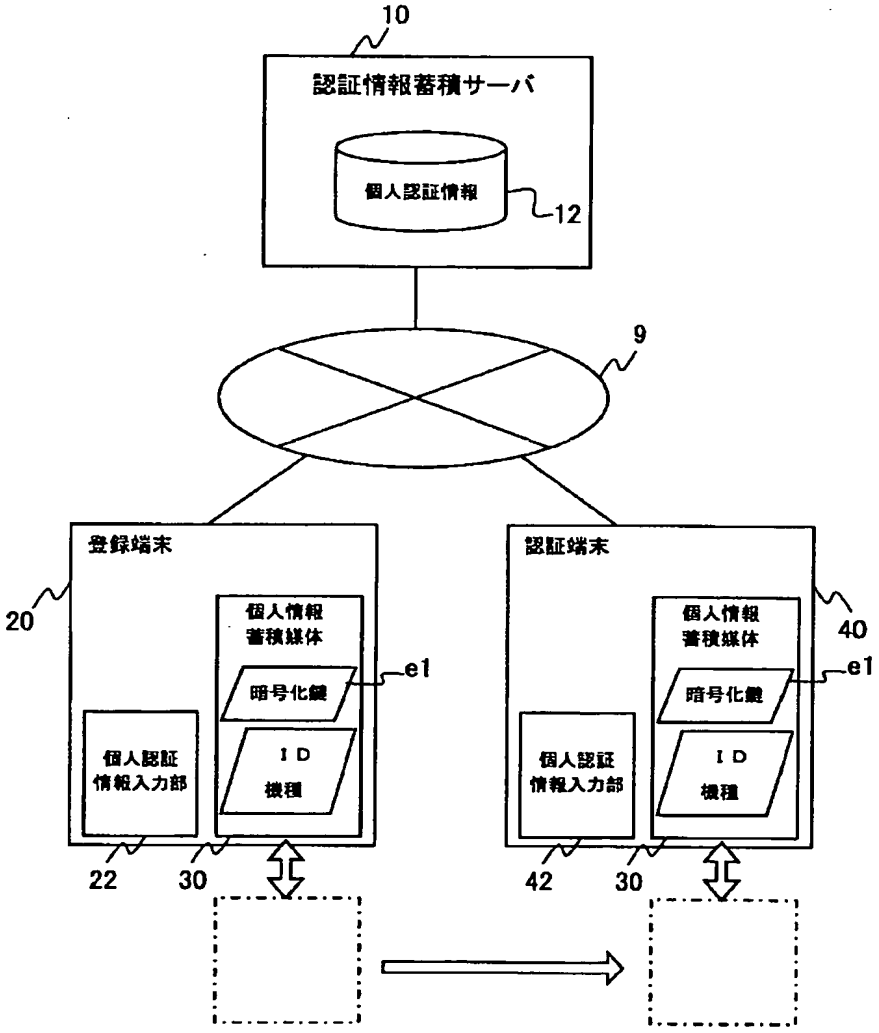
【図８】　実施の形態５にかかる認証システムの概略構成を示すブロック図である。

【図９】　実施の形態６にかかる認証システムの概略構成を示すブロック図である。

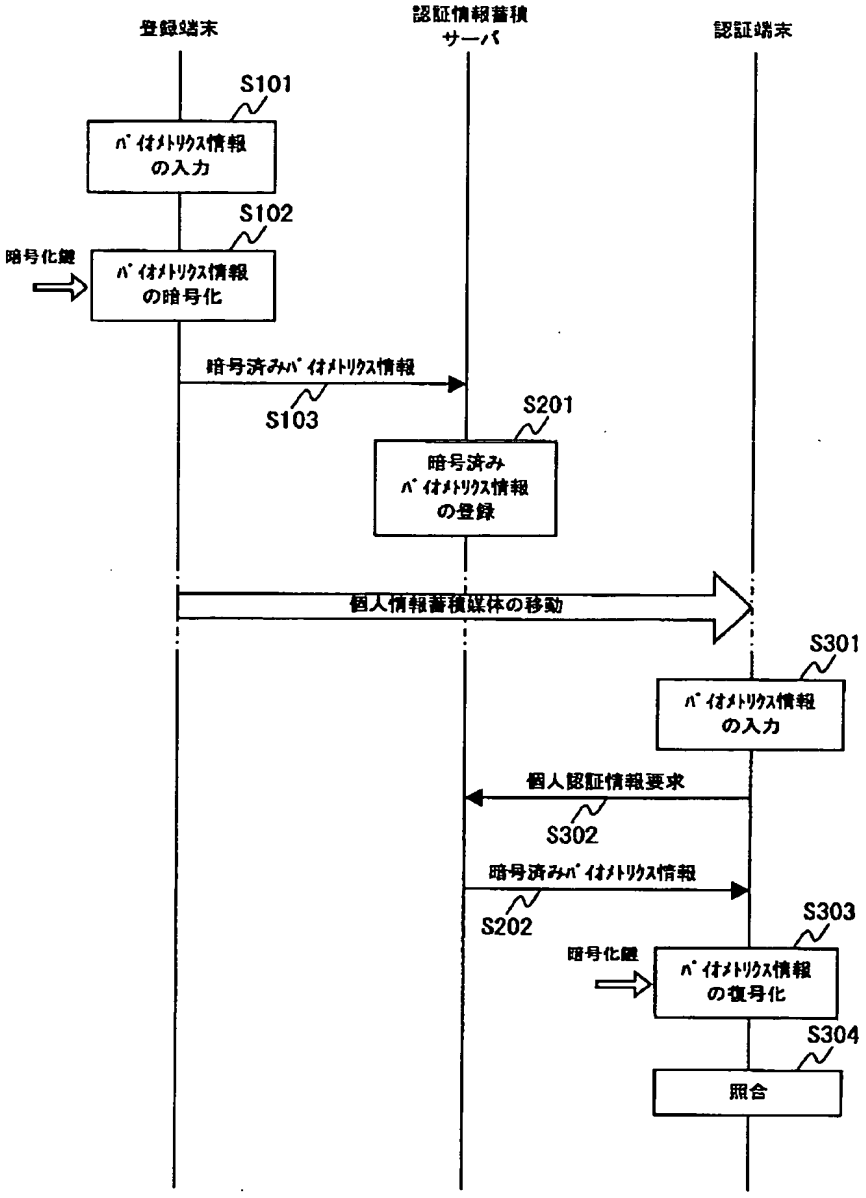
【符号の説明】

９　通信回線、１０，１００　認証情報蓄積サーバ、１２　個人認証情報データベース、２０，１２０　登録端末、２２　個人認証情報入力部、２２　個人認証情報入力部、３０　個人情報蓄積媒体、４０，１４０　認証端末、４２，１４２　個人認証情報入力部、５０　アプリケーションサーバ、１００　認証情報蓄積サーバ、１２２　個人認証情報入力部、１２４　認証情報分割部、１４４　認証情報併合部。

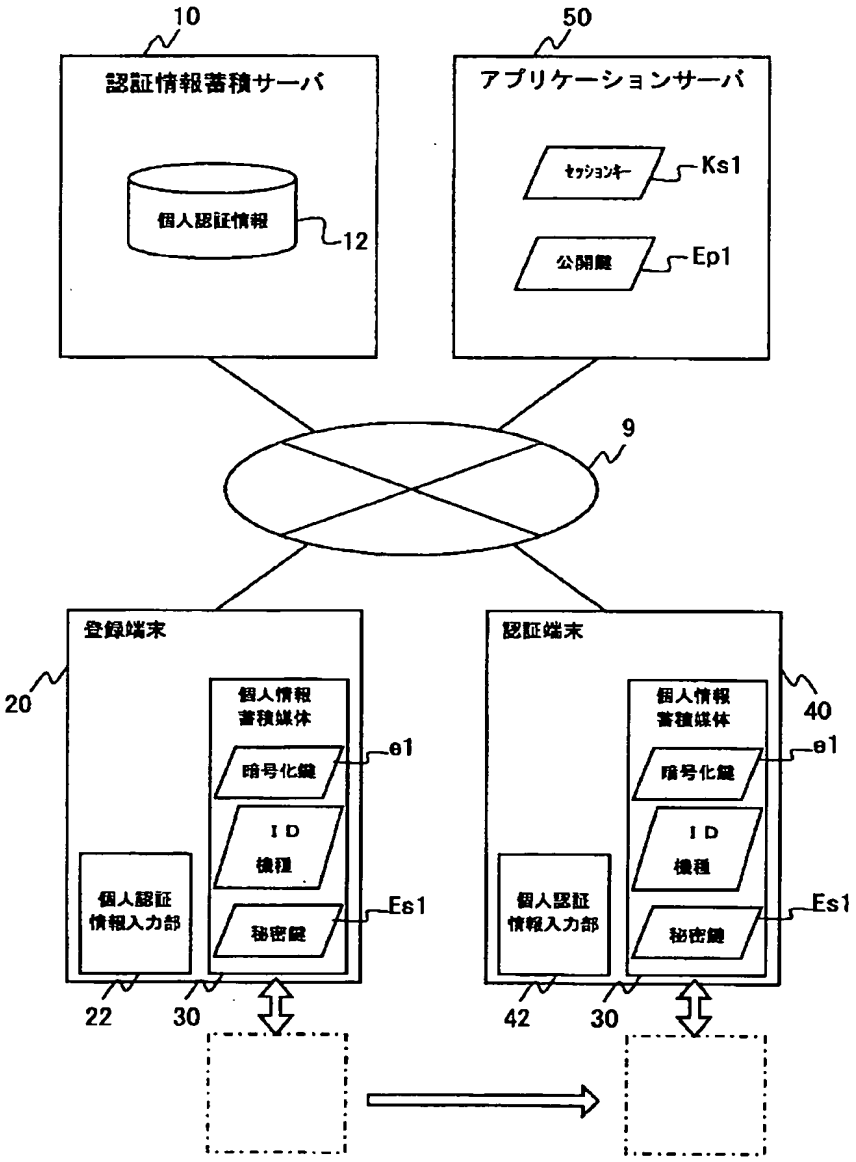
【図１】


10
認証情報蓄積サーバ
個人認証情報
12
9
登録端末
20
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
個人認証
情報入力部
22
30
認証端末
40
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
個人認証
情報入力部
42
30

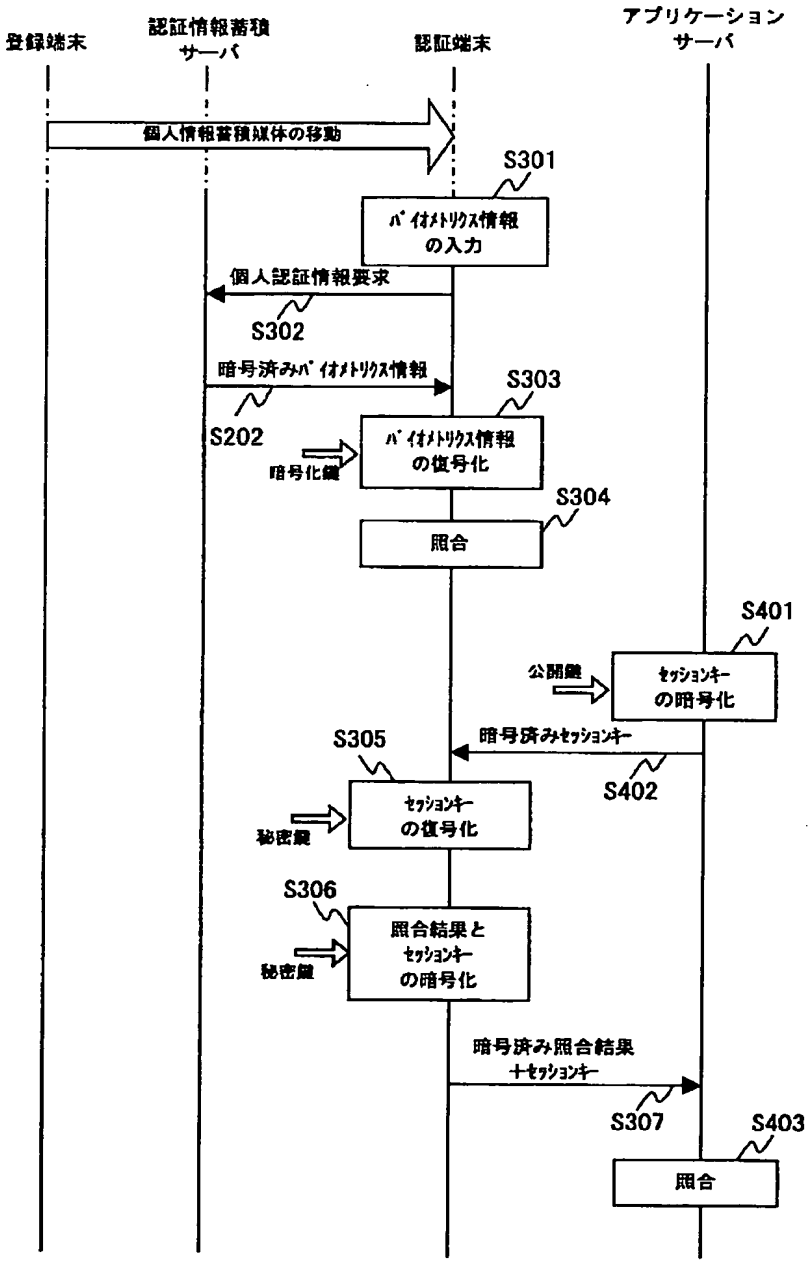
【図２】


登録端末
認証情報蓄積サーバ
認証端末
S101
バイオメトリクス情報の入力
S102
暗号化鍵
バイオメトリクス情報の暗号化
暗号済みバイオメトリクス情報
S103
S201
暗号済みバイオメトリクス情報の登録
個人情報蓄積媒体の移動
S301
バイオメトリクス情報の入力
個人認証情報要求
S302
暗号済みバイオメトリクス情報
S202
S303
暗号化鍵
バイオメトリクス情報の復号化
S304
照合

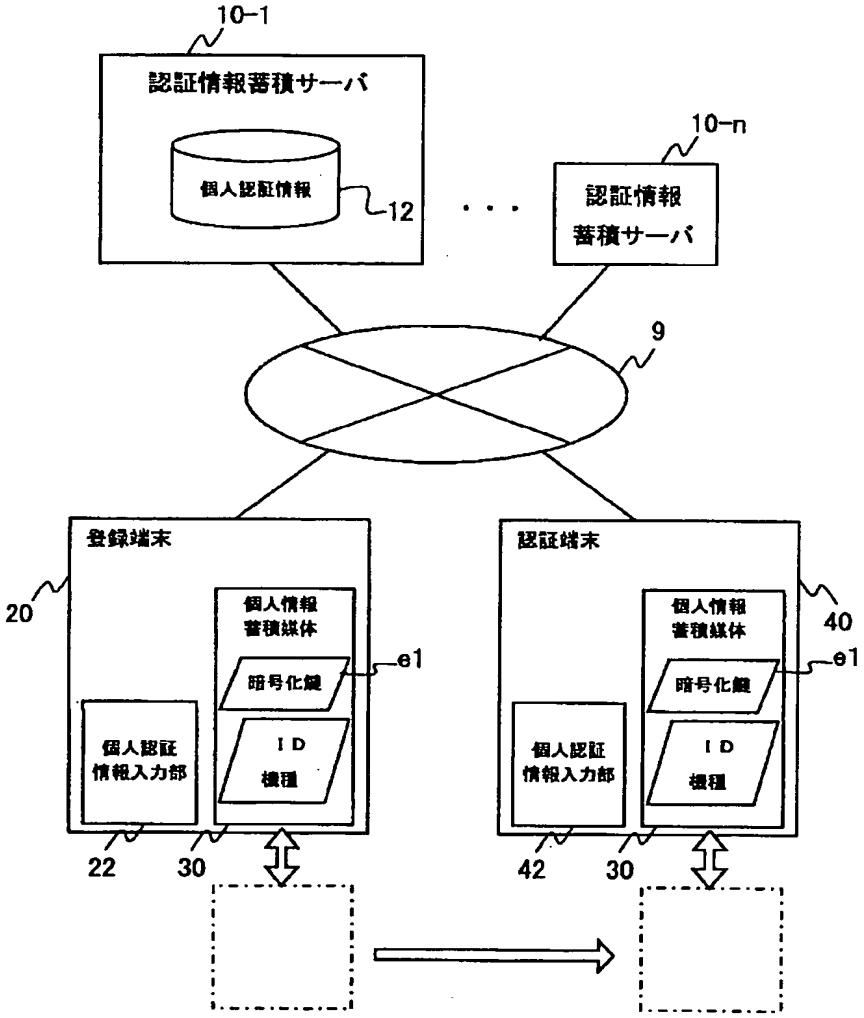
【図３】


10
認証情報蓄積サーバ
個人認証情報
12
50
アプリケーションサーバ
セッションキー
Ks1
公開鍵
Ep1
9
登録端末
20
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
秘密鍵
Es1
個人認証
情報入力部
22
30
認証端末
40
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
秘密鍵
Es1
個人認証
情報入力部
42
30

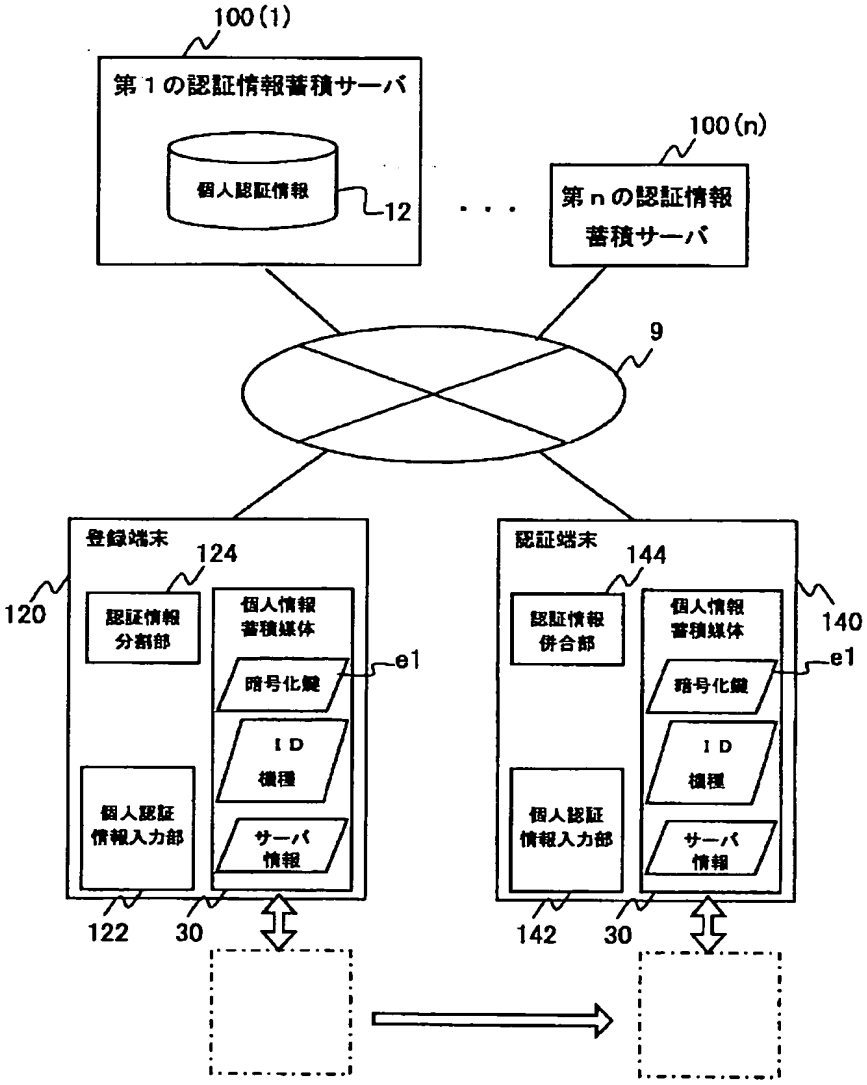
【図４】


登録端末
認証情報蓄積サーバ
認証端末
アプリケーションサーバ
個人情報蓄積媒体の移動
S301
バイオメトリクス情報の入力
個人認証情報要求
S302
暗号済みバイオメトリクス情報
S303
S202
暗号化鍵
バイオメトリクス情報の復号化
S304
照合
S401
公開鍵
セッションキーの暗号化
暗号済みセッションキー
S305
S402
セッションキーの復号化
秘密鍵
S306
照合結果とセッションキーの暗号化
秘密鍵
暗号済み照合結果＋セッションキー
S307
S403
照合

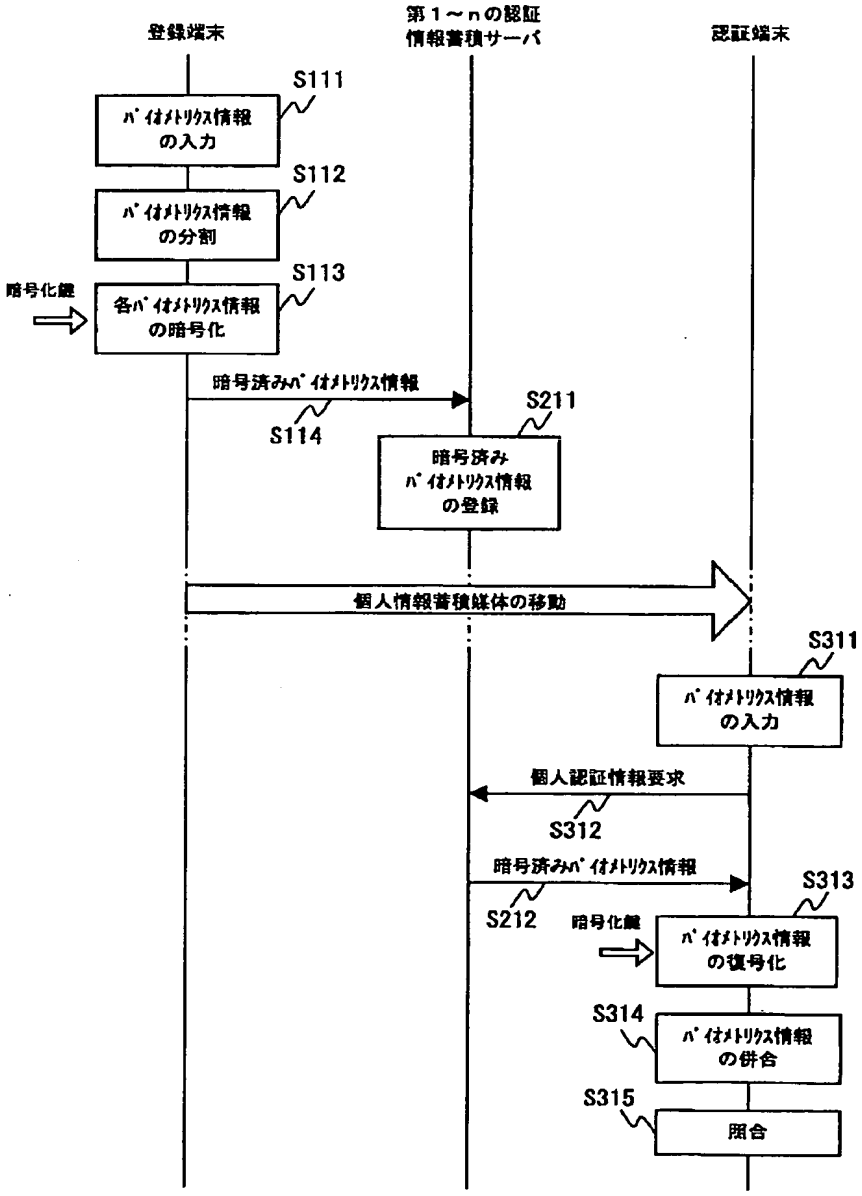
【図５】


10-1
認証情報蓄積サーバ
個人認証情報
12
10-n
認証情報
蓄積サーバ
9
登録端末
20
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
個人認証
情報入力部
22
30
認証端末
40
個人情報
蓄積媒体
暗号化鍵
e1
ＩＤ
機種
個人認証
情報入力部
42
30

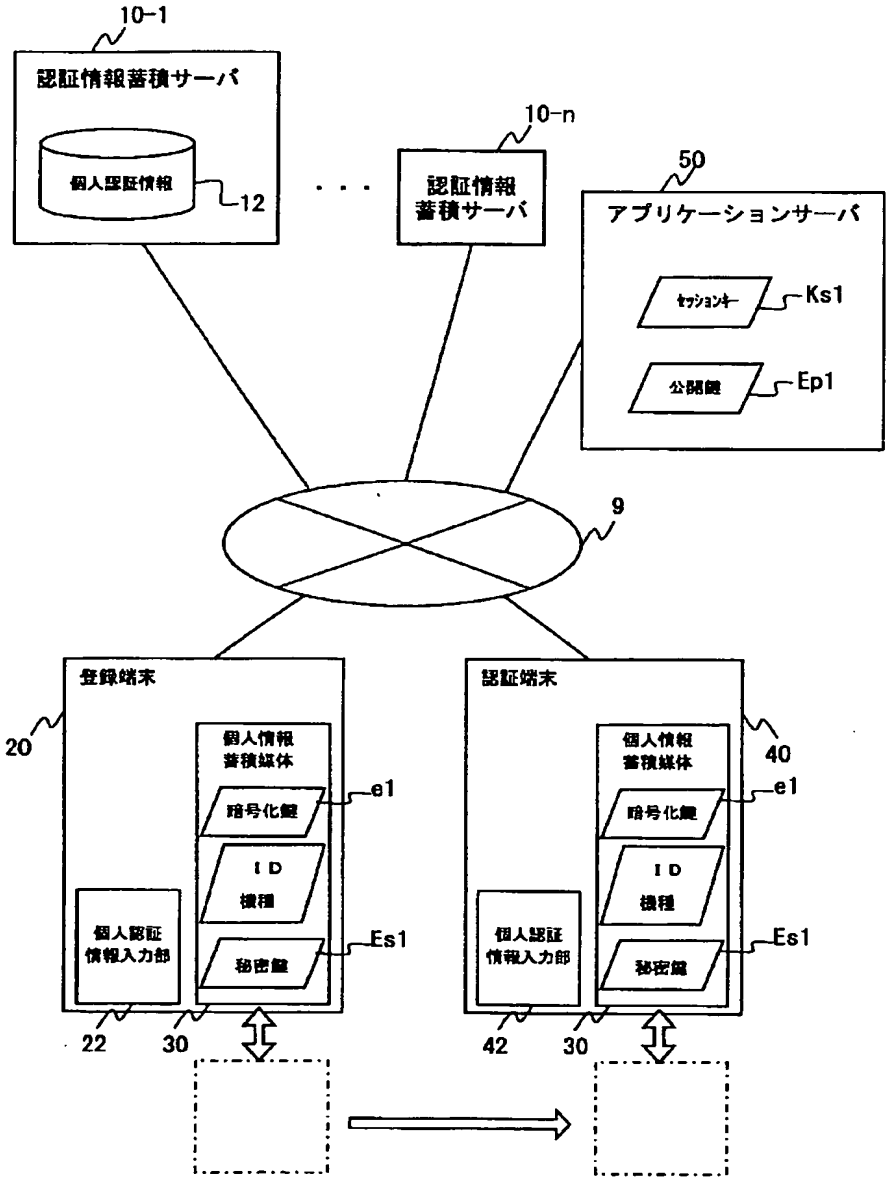
【図６】


100(1)
第１の認証情報蓄積サーバ
個人認証情報
12
100(n)
第ｎの認証情報蓄積サーバ
9
登録端末
120
124
認証情報分割部
個人情報蓄積媒体
暗号化鍵
e1
ＩＤ
模様
サーバ情報
個人認証情報入力部
122
30
認証端末
144
認証情報併合部
個人情報蓄積媒体
暗号化鍵
e1
ＩＤ
模様
サーバ情報
個人認証情報入力部
140
142
30

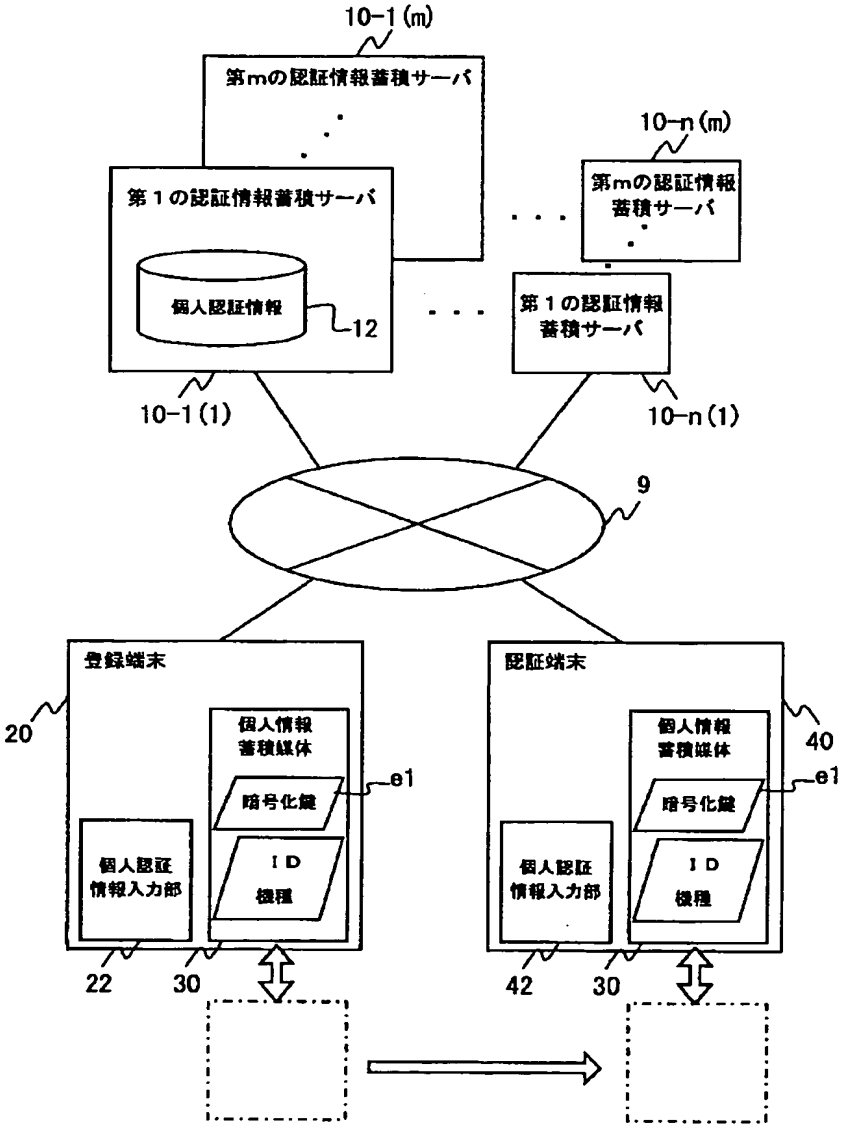
【図７】


登録端末
第１～ｎの認証情報蓄積サーバ
認証端末
S111
バイオメトリクス情報の入力
S112
バイオメトリクス情報の分割
暗号化鍵
S113
各バイオメトリクス情報の暗号化
暗号済みバイオメトリクス情報
S114
S211
暗号済みバイオメトリクス情報の登録
個人情報蓄積媒体の移動
S311
バイオメトリクス情報の入力
個人認証情報要求
S312
暗号済みバイオメトリクス情報
S212
S313
暗号化鍵
バイオメトリクス情報の復号化
S314
バイオメトリクス情報の併合
S315
照合

【図８】


10-1
認証情報蓄積サーバ
個人認証情報
12
10-n
認証情報
蓄積サーバ
50
アプリケーションサーバ
セッションキー
Ks1
公開鍵
Ep1
9
登録端末
20
個人情報
蓄積媒体
暗号化鍵
e1
ID
機種
秘密鍵
Es1
個人認証
情報入力部
22
30
認証端末
40
個人情報
蓄積媒体
暗号化鍵
e1
ID
機種
秘密鍵
Es1
個人認証
情報入力部
42
30

【図９】



フロントページの続き

(51)Int.Cl.'	識別記号	Ｆ Ｉ	テーマコード (参考)
		Ｈ０４Ｌ　9/00	６７５Ｄ

(72)発明者　鹿井　正博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

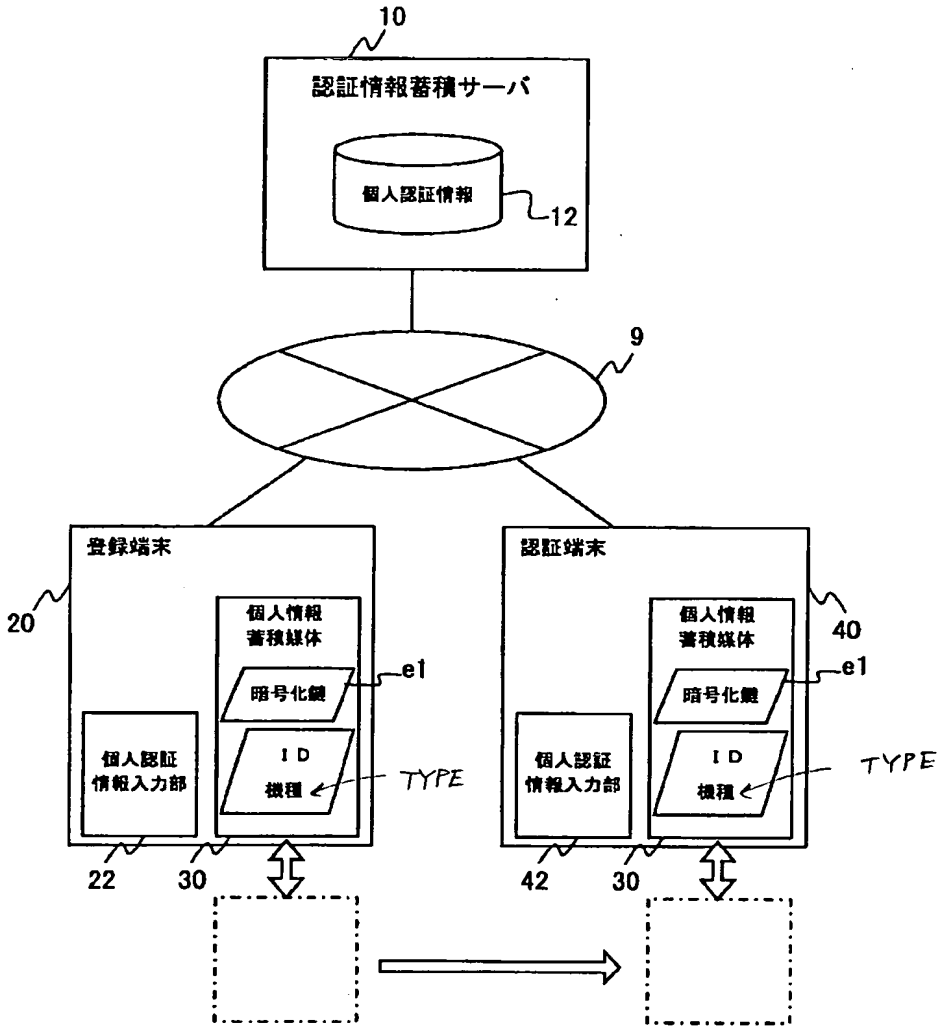
(72)発明者　白附　晶英
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　岡　徹
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　田壷　宏和
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　蔦田　広幸
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Ｆターム(参考)　5B035 AA13 BB02 BB09 BC01
5B058 CA31 KA31 KA35 KA37 KA38
5B085 AA01 AE11 AE25 AE29
5J104 AA07 AA16 EA06 EA19 KA01
KA16 KA17 KA19 MA04 NA02
NA03 NA34 NA35 NA36 NA37
PA07 PA10

FIG. 1

【図１】



9 --- COMMUNICATION LINE

10 --- AUTHENTICATION INFORMATION STORING SERVER

12 --- PERSONAL AUTHENTICATION INFORMATION

20 --- REGISTERING TERMINAL

22, 42 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT

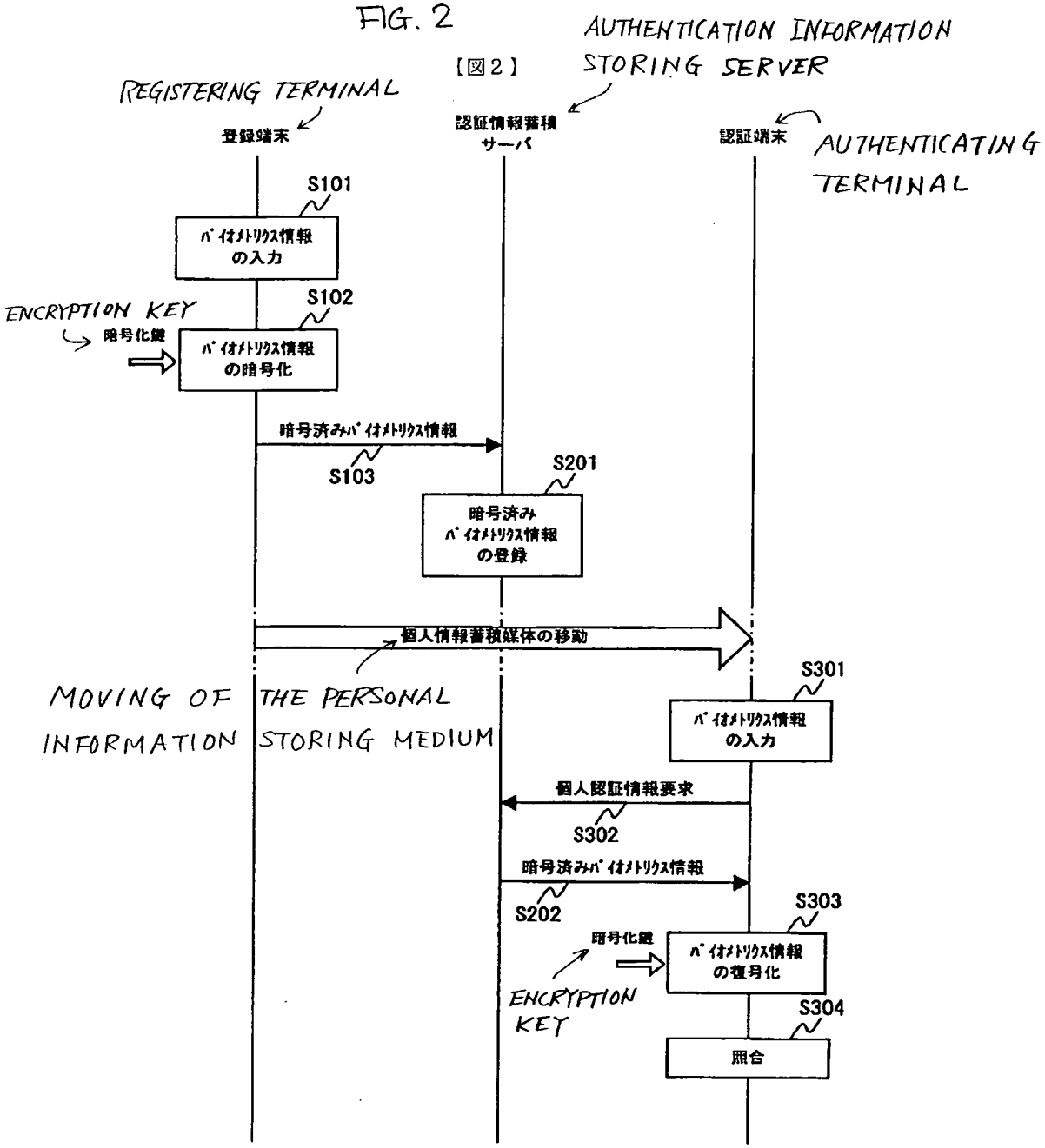
30 --- PERSONAL INFORMATION STORAGE MEDIUM

40 --- AUTHENITCATING TERMINAL

e1 --- ENCRYPTION KEY

FIG. 2

【図2】

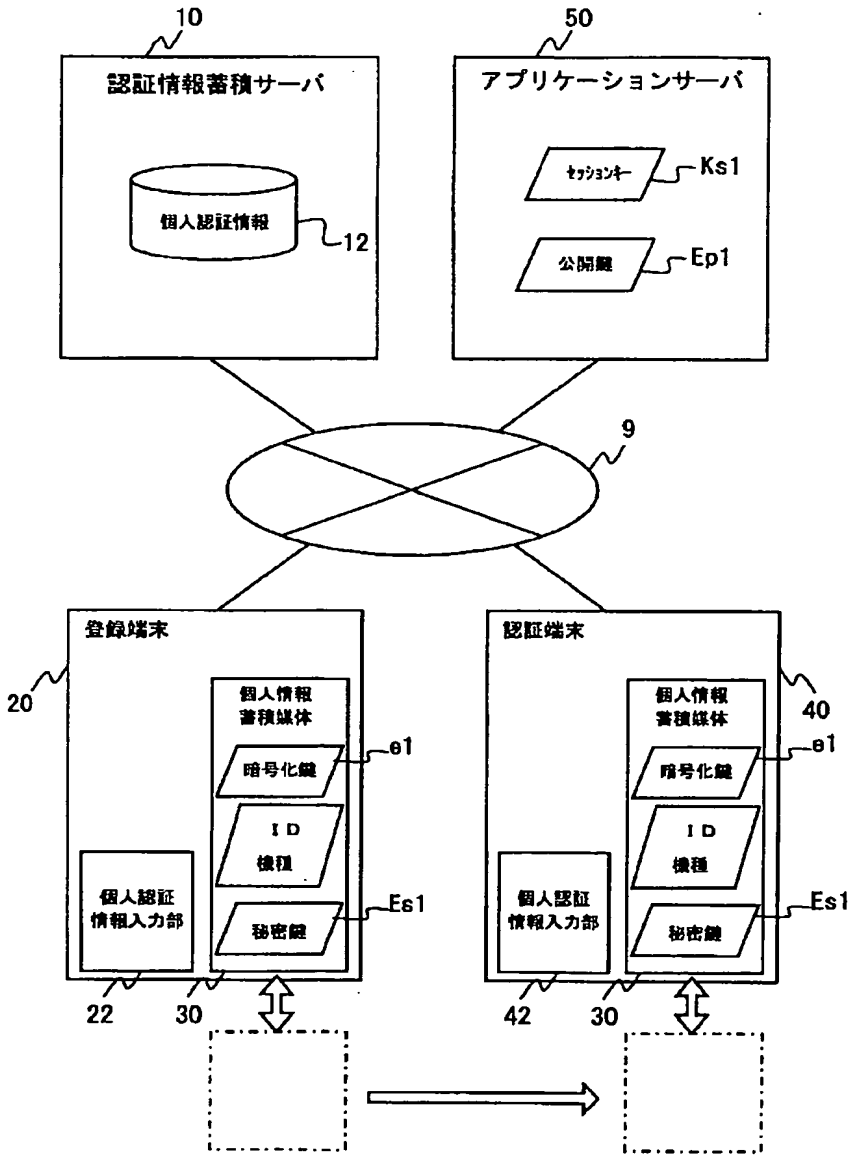


S101 --- INPUT A BIOMETRICS INFORMATION
S102 --- ENCRYPT THE BIOMETRICS INFORMATION
S103 --- ENCRYPTED BIOMETRICS INFORMATION
S201 --- REGISTER THE ENCRYPTED BIOMETRICS INFORMATION
S202 --- ENCRYPTED BIOMETRICS INFORMATION
S301 --- INPUT THE BIOMETRICS INFORMATION
S303 --- DECRYPT THE BIOMETRICS INFORMATION
S304 --- COMPARING

e1 --- ENCRYPTION KEY
Es1 --- PRIVATE KEY
50 --- APPLICATION SERVER
Ks1 --- SESSION KEY
Ep1 --- PUBLIC KEY

FIG. 3

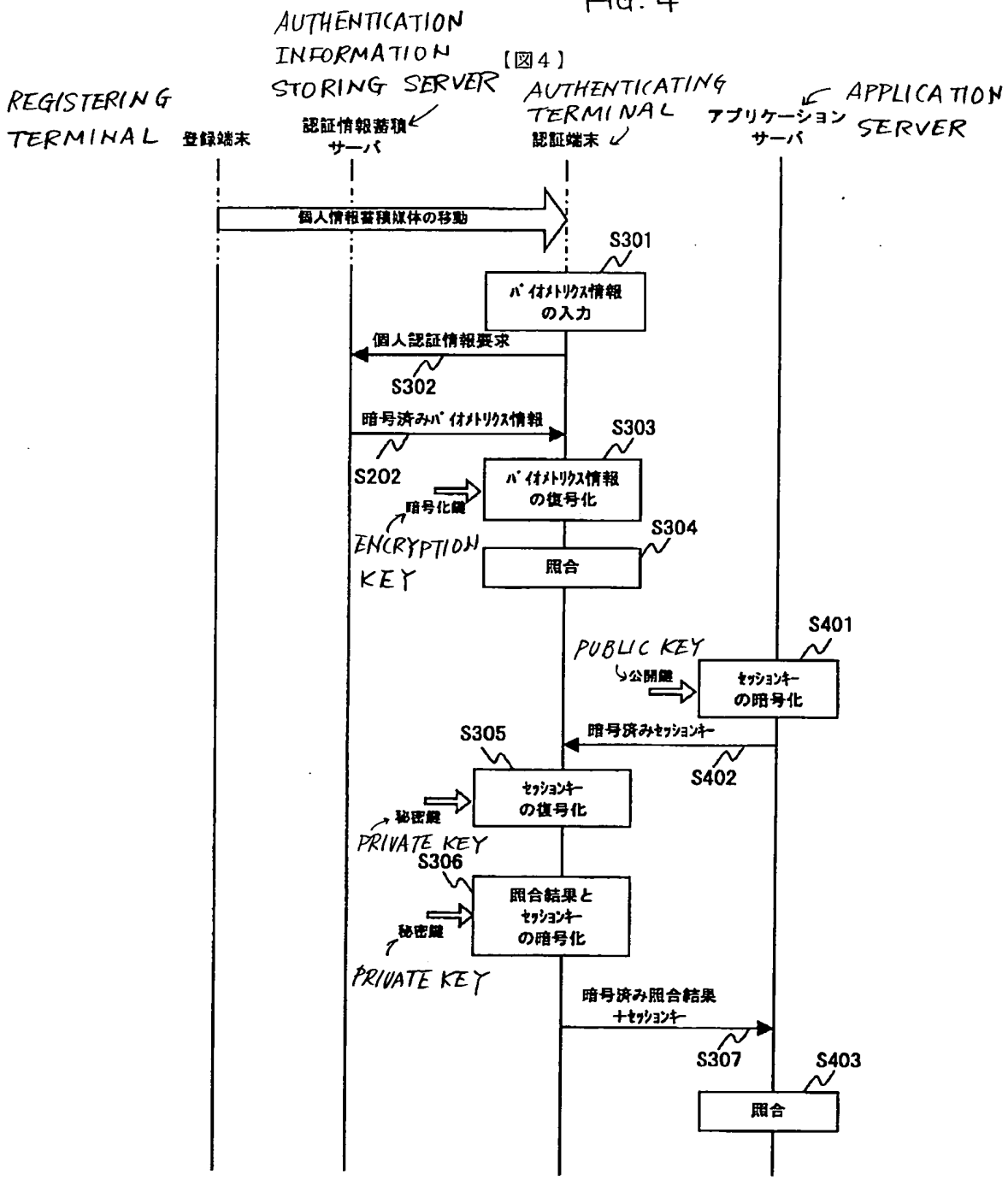
【図３】



9 --- COMMUNICATION LINE
10 --- AUTHENTICATION INFORMATION STORING SERVER
12 --- PERSONAL AUTHENTICATION INFORMATION
20 --- REGISTERING TERMINAL
22, 42 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT
30 --- PERSONAL INFORMATION STORAGE MEDIUM
40 --- AUTHENITCATING TERMINAL

FIG. 4

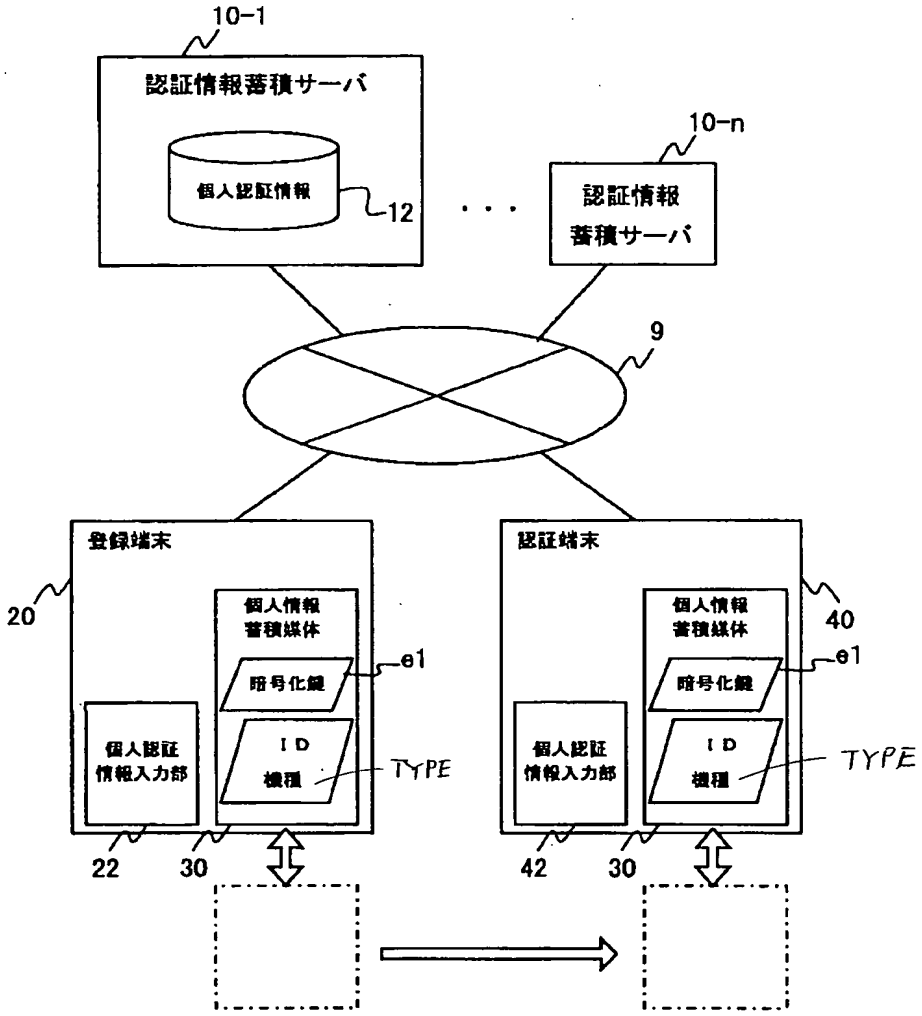
【図４】



S202 --- ENCRYPTED BIOMETRICS INFORMATION
S301 --- INPUT THE BIOMETRICS INFORMATION
S302 --- REQUEST FOR PERSONAL AUTHENTICATION
S303 --- DECRYPT THE BIOMETRICS INFORMATION
S304 --- COMPARING
S305 --- DECRYPT THE SESSION KEY
S306 --- RESULT OF COMPARISON AND ENCRYPTION OF THE SESSION KEY
S307 --- ENCRYPTED RESULT OF COMPARISON AND SESSION KEY
S401 --- ENCRYPT A SESSION KEY
S402 --- ENCRYPTED SESSION KEY
S403 --- COMPARING

FIG. 5

【図５】



9 --- COMMUNICATION LINE

10-1 - 10-n --- AUTHENTICATION INFORMATION STORING SERVER

12 --- PERSONAL AUTHENTICATION INFORMATION

20 --- REGISTERING TERMINAL

22, 42 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT

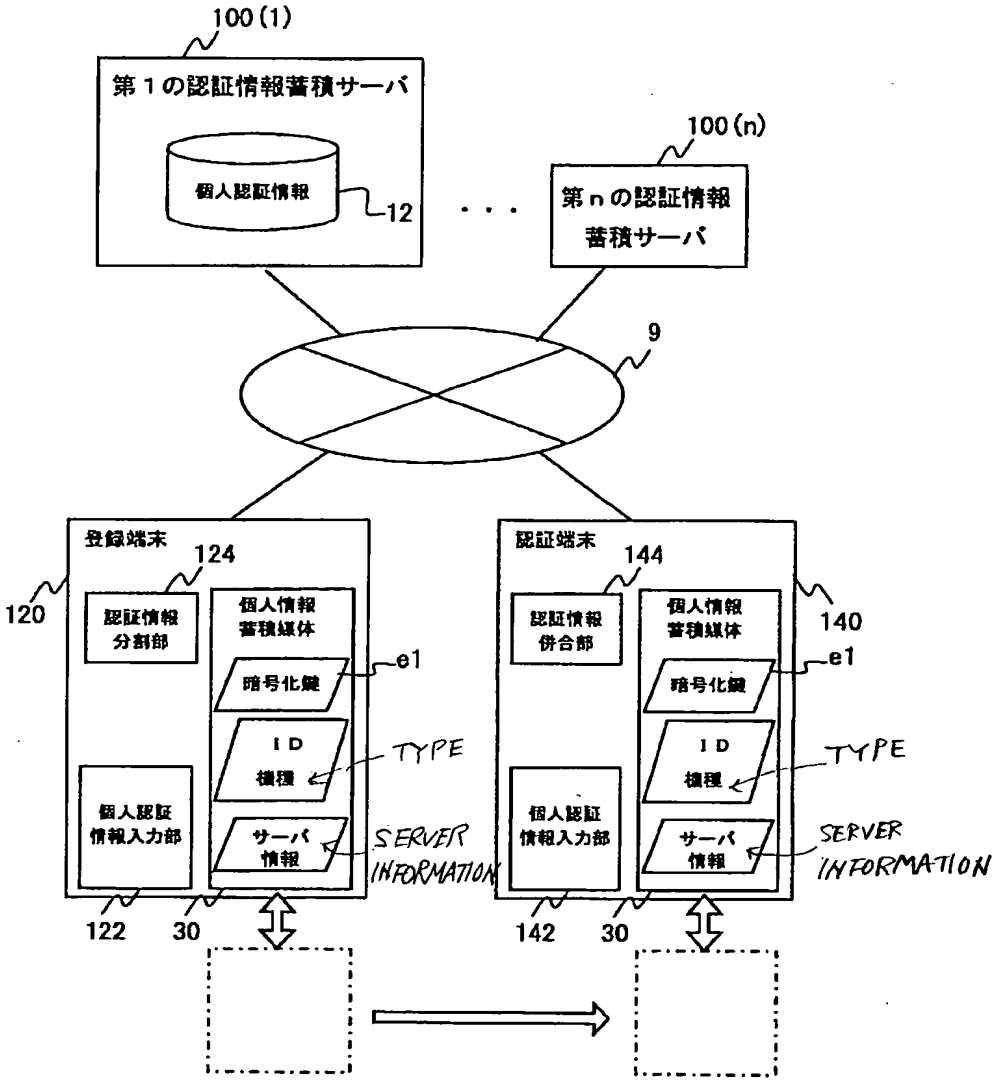
30 --- PERSONAL INFORMATION STORAGE MEDIUM

40 --- AUTHENITCATING TERMINAL

e1 --- ENCRYPTION KEY

FIG. 6

【図６】



9 --- COMMUNICATION LINE

100(1) --- FIRST AUTHENTICATION INFORMATION STORING SERVER

100(N) --- N-th AUTHENTICATION INFORMATION STORING SERVER

12 --- PERSONAL AUTHENTICATION INFORMATION

120 --- REGISTERING TERMINAL

122, 142 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT

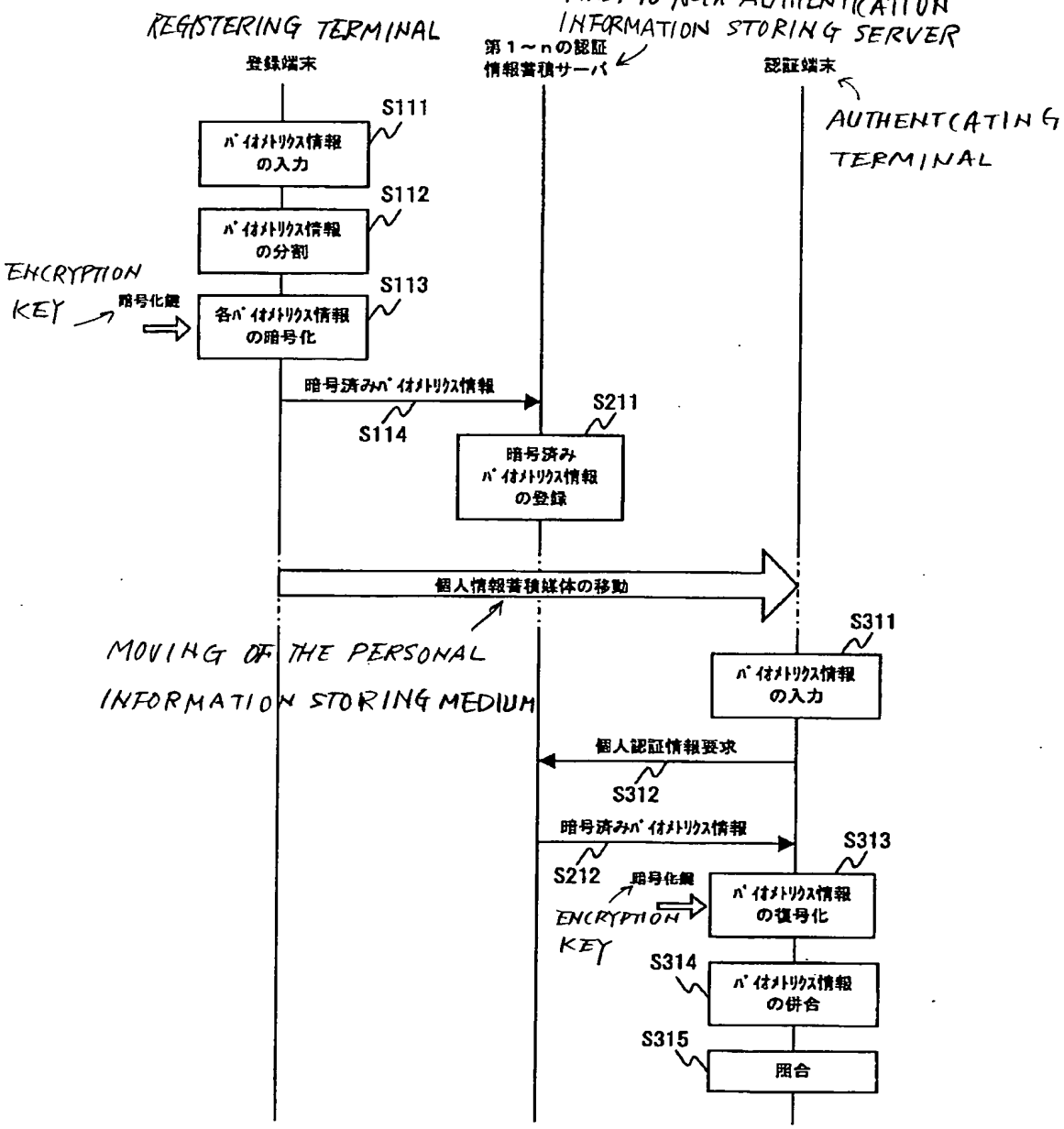
30 --- PERSONAL INFORMATION STORAGE MEDIUM

140 --- AUTHENITCATING TERMINAL

e1 --- ENCRYPTION KEY

FIG. 7

【図7】 FIRST TO N-th AUTHENTICATION INFORMATION STORING SERVER



S111 --- INPUT A BIOMETRICS INFORMATION

S112 --- DIVIDE THE BIOMETRICS INFORMATION

S113 --- ENCRYPT EACH OF THE BIOMETRICS INFORMATION

S114 --- ENCRYPTED BIOMETRICS INFORMATION

S211 --- REGISTER THE ENCRYPTED BIOMETRICS INFORMATION

S212 --- ENCRYPTED BIOMETRICS INFORMATION

S311 --- INPUT THE BIOMETRICS INFORMATION

S312 --- REQUEST FOR TRANSMITTING A PERSONAL AUTHENTICATION

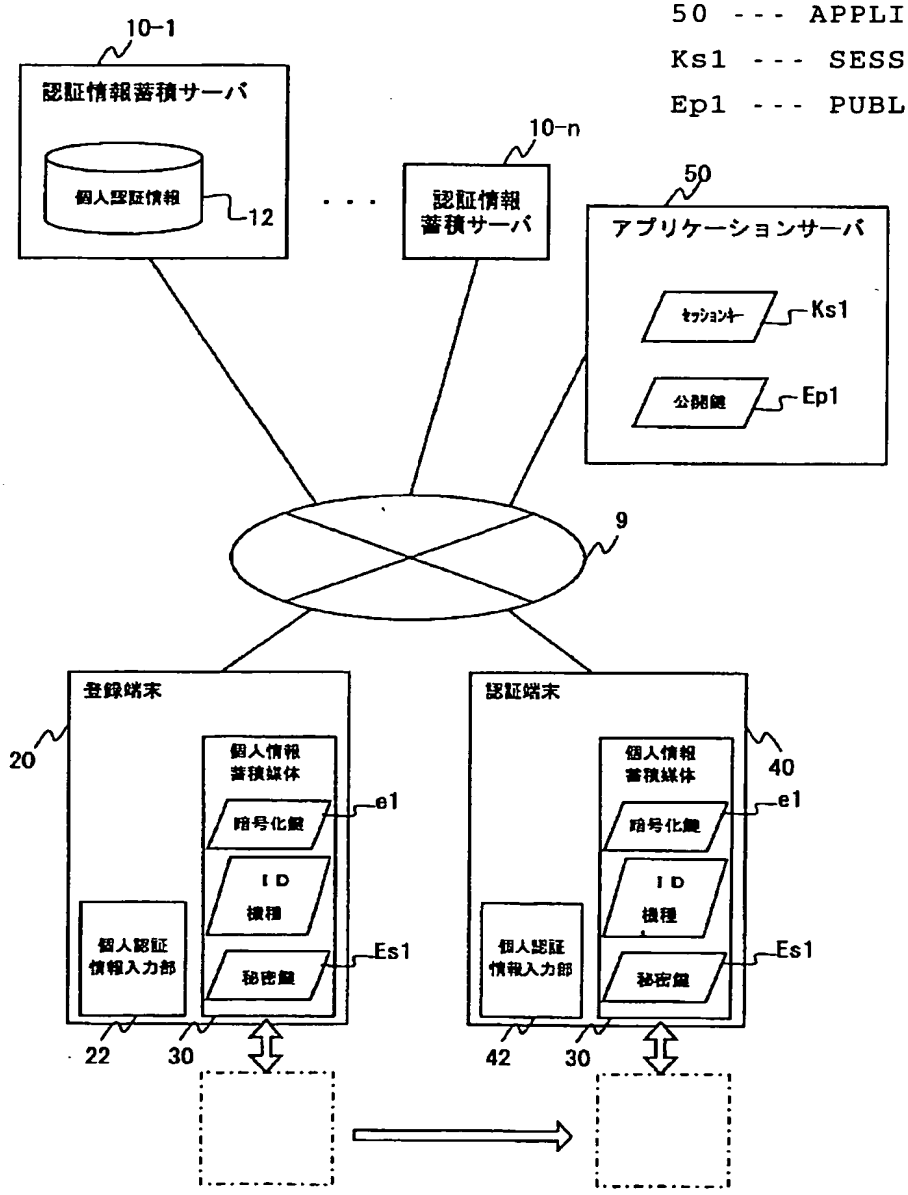
S313 --- DECRYPT THE BIOMETRICS INFORMATION

S314 --- MERGE EACH OF THE BIOMETRICS INFORMATION

S315 --- COMPARING

FIG. 8

【図8】



e1 --- ENCRYPTION KEY

Es1 --- PRIVATE KEY

50 --- APPLICATION SERVER

Ks1 --- SESSION KEY

Ep1 --- PUBLIC KEY

9 --- COMMUNICATION LINE

10-1 --- AUTHENTICATION INFORMATION STORING SERVER

10-n --- AUTHENTICATION INFORMATION STORING SERVER

12 --- PERSONAL AUTHENTICATION INFORMATION

20 --- REGISTERING TERMINAL

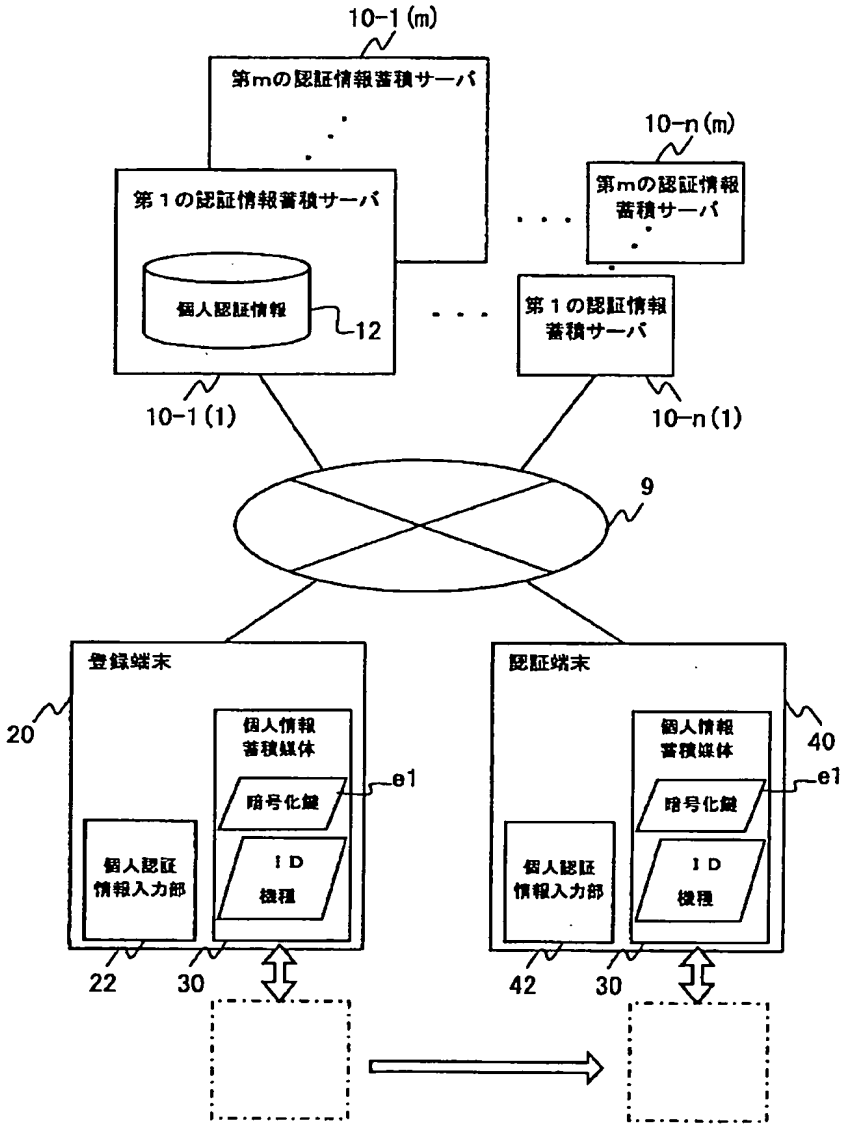
22, 42 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT

30 --- PERSONAL INFORMATION STORAGE MEDIUM

40 --- AUTHENITCATING TERMINAL

FIG. 9

【図９】



9 --- COMMUNICATION LINE

10-1(1) --- FIRST AUTHENTICATION INFORMATION STORING SERVER

10-1(m) --- M-th AUTHENTICATION INFORMATION STORING SERVER

10-n(1) --- FIRST AUTHENTICATION INFORMATION STORING SERVER

10-n(m) --- M-th AUTHENTICATION INFORMATION STORING SERVER

12 --- PERSONAL AUTHENTICATION INFORMATION

20 --- REGISTERING TERMINAL

22, 42 --- PERSONAL AUTHENTICATION INFORMATION INPUT UNIT

30 --- PERSONAL INFORMATION STORAGE MEDIUM

40 --- AUTHENITCATING TERMINAL

e1 --- ENCRYPTION KEY

2002-297551

[SCOPE OF CLAIMS]

[CLAIM 1] An authentication system comprising:

a personal information storage medium in which at least an encryption key is recorded;

a registering terminal on which user biometric information is input, and which encrypts said input biometric information by using said encryption key read out of said personal information storage medium and transmits said encrypted biometric information;

an authentication information storing server which receives said encrypted biometric information transmitted from said registering terminal, stores said received encrypted biometric information, and transmits said stored biometric information upon request; and

an authenticating terminal on which user biometric information is input, and which receives said encrypted biometric information from said authentication information storing server, decrypts said received encrypted biometric information by using said encryption key read out of said personal information storage medium, and compares said decrypted biometric information with said input biometric information, wherein

said registering terminal, said authentication information storing server, and said authenticating terminal are connected via a communication line.

[CLAIM 2] An authentication system comprising:

a personal information storage medium in which at least an encryption key and a private key are recorded;

a registering terminal on which user biometric information is input, and which encrypts said input biometric information by using said encryption key read out of said personal information storage medium and transmits said encrypted biometric information;

an authentication information storing server which receives said encrypted biometric information transmitted

from said registering terminal, stores said received encrypted biometric information, and transmits said stored biometric information upon request;

an authenticating terminal on which user biometric information is input, and which receives said encrypted biometric information from said authentication information storing server, decrypts said received encrypted biometric information by using said encryption key read out of said personal information storage medium, compares said decrypted biometric information with said input biometric information and outputs a comparison result, receives a session key encrypted by a public key to be paired with said private key, decrypts said received encrypted session key by using said private key read out of said personal information storage medium, encrypts said decrypted session key and said comparison result by using said private key, and transmits said encrypted session key and comparison result; and

an application server which provides services such as electronic commerce and acquires said public key to be paired with said private key, and which, when requesting user authentication from said authenticating terminal, generates said session key, encrypts said generated session key by using said public key, transmits said encrypted session key to said authenticating terminal, and receives said encrypted session key and comparison result from said authenticating terminal, wherein

said registering terminal, said authentication information storing server, said authenticating terminal, and said application server are connected via a communication line.

[CLAIM 3] An authentication system comprising:

a personal information storage medium in which at least an encryption key is recorded;

a registering terminal on which user first biometric information is input, and which divides said input first biometric information into a plurality of pieces of second

biometric information, encrypts each of said plurality of pieces of second biometric information by using said encryption key read out of said personal information storage medium, and transmits said encrypted pieces of second biometric information;

a plurality of authentication information storing servers which respectively receive said encrypted pieces of second biometric information transmitted from said registering terminal, store said received encrypted pieces of second biometric information, and transmit said stored pieces of second biometric information upon request; and

an authenticating terminal on which user biometric information is input, and which receives said encrypted pieces of second biometric information from said plurality of authentication information storing servers, decrypts said received encrypted pieces of second biometric information by using said encryption key read out of said personal information storage medium, reconstructs said first biometric information by merging together said decrypted pieces of second biometric information, and compares said reconstructed biometric information with said input biometric information, wherein

said registering terminal, said authentication information storing servers, and said authenticating terminal are connected via a communication line.

[CLAIM 4] An authentication system comprising:

a personal information storage medium in which at least an encryption key and a private key are recorded;

a registering terminal on which user first biometric information is input, and which divides said input first biometric information into a plurality of pieces of second biometric information, encrypts each of said plurality pieces of second biometric information by using said encryption key read out of said personal information storage medium, and transmits said encrypted pieces of second biometric information;

a plurality of authentication information storing servers which respectively receive said encrypted pieces of second biometric information transmitted from said registering terminal, store said received encrypted pieces of second biometric information, and transmit said stored pieces of second biometric information upon request; and

an authenticating terminal on which user biometric information is input, and which receives said encrypted pieces of second biometric information from said plurality of authentication information storing servers, decrypts said received encrypted pieces of second biometric information by using said encryption key read out of said personal information storage medium, reconstructs said first biometric information by merging together said decrypted pieces of second biometric information, compares said reconstructed biometric information with said input biometric information and outputs a comparison result, receives a session key encrypted by a public key to be paired with said private key, decrypts said received encrypted session key by using said private key read out of said personal information storage medium, encrypts said decrypted session key and said comparison result by using said private key, and transmits said encrypted session key and comparison result; and

an application server which provides services such as electronic commerce and acquires said public key to be paired with said private key, and which, when requesting user authentication from said authenticating terminal, generates said session key, encrypts said generated session key by using said public key, transmits said encrypted session key to said authenticating terminal, and receives said encrypted session key and comparison result from said authenticating terminal, wherein

said registering terminal, said authentication information storing servers, said authenticating terminal, and said application server are connected via a communication line.

[CLAIM 5] An authentication system as claimed in any one of claims 1 to 4, wherein said authentication system includes a plurality of mirror servers each of which stores biometric information whose contents are identical to the contents of the biometric information stored in said authentication information storing server, and wherein

said registering terminal transmits said encrypted biometric information to said authentication information storing server or to any one of said plurality of mirror servers, and

said authenticating terminal receives said encrypted biometric information from said authentication information storing server or from any one of said plurality of mirror servers.

[Problems to be Solved by the Invention] However, in the above-described user authentication using digital signatures, once a digital signature is registered in a user terminal such as a computer, it is only required to enter a password at the time of user authentication; therefore, if the password becomes known to a person other than the legitimate user, there is no way to prevent that person from masquerading at the user terminal. That is, the association between the legitimate user and the digital signature is necessary only when acquiring the digital signature from a certification authority or the like, and no protection has been provided against social hacking such as password leakage.

[0010] On the other hand, the "Remote Authentication System" disclosed in Japanese Unexamined Patent Publication No. 2000-092046 has had the problem that, as the biometric information can be decrypted at the authenticating server side, the information cannot be fully protected if a malicious operation is performed at the server side.

[0011] Here, the biometric information to be compared against, that is, the registered biometric information, could

be recorded in a transportable recording medium, but this would not be realistic because the size of biometric information is generally very large compared with a digital signature and hence requires the use of a large-capacity recording medium. Furthermore, if the recording medium is stolen, there is a substantial risk of the biometric information being analyzed, increasing the threat of masquerading.

[0012] The present invention has been devised to solve the above problems, and an object of the invention is to achieve an authentication system that enables user authentication to be performed in a secure and reliable manner even between different terminals.

[Embodiments of the Invention] Embodiments of an authentication system according to the present invention will be described in detail below with reference to the drawings. Here, it should be understood that the present invention is in no way limited by the specific embodiments described herein.

[0024] Embodiment 1. First, an authentication system according to a first embodiment will be described. The authentication system of the first embodiment is characterized in that, using a registering terminal, biometric information such as a user's fingerprint, iris, or handwriting is encrypted and registered in advance with an authentication information storing server and, at the same time, its encryption and decryption key information, registering terminal type information, and user ID information are recorded in a transportable personal information storage medium, and in that when performing authentication on an authenticating terminal, the encrypted biometric information obtained from the authentication information storing server is decrypted using the encryption key recorded in the personal information storage medium, and the decrypted biometric information is compared with newly

input biometric information to authenticate the identity of the user.

[0025] Figure 1 is a block diagram showing in simplified form the configuration of the authentication system according to the first embodiment. In Figure 1, the authentication system of the first embodiment comprises an authentication information storing server 10, a registering terminal 20, and an authenticating terminal 40, which are connected via a communication line 9 so as to be able to communicate with each other.

[0026] The authentication information storing server 10 is similar in configuration to an Web server on the Internet, and is actually a conventional computer system. However, the authentication information storing server 10 here is configured to register and store the personal authentication information transmitted from the registering terminal 20, and to transmit the stored personal authentication information in response to a request from the authenticating terminal 40.

[0027] The registering terminal 20 is similar in configuration to a desktop computer, notebook computer, PDA (Personal Digital Assistant), portable telephone, or the like, that can use various kinds of services such as electronic commerce provided via the communication line 9, and includes a personal authentication information input section 22 on which biometric information can be input and a personal information storage medium 30.

[0028] The authenticating terminal 40 includes, in addition to the personal information storage medium 30, a personal authentication information input section 42 similar in configuration to the personal authentication information input section 22 of the registering terminal 20, the entire configuration thus being the same as that of the registering terminal 20. Accordingly, there is no particular distinction in configuration between the registering terminal 20 and the authenticating terminal 40, but it is at least required that the personal authentication information input sections 22 and

42 and the slot capable of loading the personal information storage medium 30 conform to the same specifications between the two terminals.

[0029] For example, when the user's fingerprint is input as the biometric information, the personal authentication information input sections 22 and 42 are fingerprint scanners, and when the user's handwriting is input as the biometric information, they are input pads such as tablets on which handwriting can be input using a stylus pen.

[0030] The personal information storage medium 30 is a nonvolatile storage medium that is easy to carry, for example, a magnetic card, a flash memory card, or an IC card. Accordingly, the registering terminal 20 is provided with a slot capable of loading the personal information storage medium 30.

[0031] The communication line 9 may be wired or wireless, and use may be made of a public telephone network or a leased line. The term also includes an IP network, such as the Internet, constructed over such communication lines.

[0032] The operation of the authentication system according to the first embodiment will be described below. Figure 2 is a flowchart illustrating the operation of the authentication system according to the first embodiment. In Figure 2, first the user inputs via the personal authentication information input section 22 of the registering terminal 20 the user's own biometric information that can be input on the personal authentication information input section 22 (step S101). For example, when the personal authentication information input section 22 is a fingerprint scanner, the registering terminal 20 extracts feature points based on feature point matching from the fingerprint image captured by the fingerprint scanner, and acquires the extracted feature point information as the biometric information.

[0033] Next, the registering terminal 20 applies encryption to the acquired biometric information by using a prescribed encryption key e1 (step S102). This encryption key e1 is

recorded in the personal information storage medium 30 together with the user ID information, the type information of the registering terminal 20, etc.

[0034] After that, the registering terminal 20 transmits the encrypted biometric information together with the user ID information, the type information of the registering terminal 20, etc. to the authentication information storing server 10 via the communication line 9 (step S103). Upon receiving the registration information including the encrypted biometric information, the authentication information storing server 10 registers the registration information in a personal authentication information database 12 (step S201).

[0035] When the registration of the biometric information is completed in the above procedure, the user removes the personal information storage medium 30 from the registering terminal 20, and keeps it in a safe and secure manner, for example, by carrying it with him, until it becomes necessary for authentication on the authenticating terminal 40. In particular, the personal information storage medium 30 may also be provided with the function of an ID card that is used for other authentication purposes such as when entering or leaving an access-controlled building or when using electronic money; in that case, the user is spared the necessity of carrying a plurality of recording media and the confusion when using the recording media.

[0036] Next, when using the authenticating terminal 40 which is different from the registering terminal 20, the user loads the personal information storage medium 30 into the authenticating terminal 40. Then, for the user authentication that the authenticating terminal 40 requests when the user uses the authenticating terminal 40 by itself or to receive services provided via the communication line 9, the user inputs his biometric information via the personal authentication information input section 42 of the authenticating terminal 40 in the same manner as when inputting the biometric information using the registering

terminal 20 (step S301).

[0037] The authenticating terminal 40 temporarily stores the biometric information input by the user, and transmits, together with the user ID information, the type information of the registering terminal 20, etc. recorded in the personal information storage medium 30, a request to the authentication information storing server 10 for transmission of the registered personal authentication information, that is, the encrypted biometric information (step S302).

[0038] Upon receiving the personal authentication information request from the authenticating terminal 40, the authentication information storing server 10 retrieves from the personal authentication information database 12 the encrypted biometric information that matches the user ID information, the type information of the registering terminal 20, etc. contained in the personal authentication information request, and transmits the biometric information to the authenticating terminal 40 (step S202).

[0039] When the encrypted biometric information is received from the authentication information storing server 10, the authenticating terminal 40 decrypts the encrypted biometric information by using the encryption key e1 recorded in the personal information storage medium 30 (step S303). Then, the authenticating terminal 40 compares the decrypted biometric information with the biometric information input in step S301, and determines whether they match or not (step S304).

[0040] When it is determined that they match, the authenticating terminal 40 makes a transition to a state in which the authenticating terminal 40 can be used by itself or used to receive services via the communication line 9, and displays a message or the like to that effect. Conversely, when they do not match, a message or warning or the like prompting the user to reenter biometric information is displayed.

[0041] As described above, according to the authentication

system of the first embodiment, as the preregistered biometric information is managed by the externally located authentication information storing server 10, personal authentication can be easily accomplished even when the user desires to use a terminal, for example, the authenticating terminal 40, that is different from the registering terminal 20 that the user used at the time of registration.

[0042] Furthermore, as the encryption key e1 is recorded in the personal information storage medium 30 that can be used between different terminals, the biometric information encrypted with the encryption key e1 can be decrypted using the personal information storage medium 30, which means that the biometric information can be prestored in encrypted form in the authentication information storing server 10. In other words, user authentication cannot be done on a terminal not loaded with the personal information storage medium 30, and this ensures high security.

[0043] Moreover, since the personal information storage medium 30 need only hold at least the encryption/decryption key information, a memory amount used in the personal information storage medium 30 is small even if the size of the biometric information is large. Suppose, for example, that the biometric information is fingerprint information; in this case, even when fingerprint scanners differ between a plurality of authenticating terminals, it becomes possible to perform personal authentication on any terminal by preregistering fingerprint information for each different fingerprint scanner for the same user, as long as the specification of the fingerprint scanner of the registering terminal 20 matches that of the fingerprint scanner of the authenticating terminal 40.

[0044] This also means that not only the same kind of biometric information but also different kinds of biometric information can be used by preregistering them for the same user. For example, when fingerprint information and handwriting information for the same user are preregistered

in encrypted form with the authentication information storing server 10, user authentication can be done on a terminal equipped with an input pad as well as on a terminal equipped with a fingerprint scanner. That is, by using the registering terminal type information, a plurality of different authentication mechanisms can be used selectively.

[0045] Embodiment 2. Next, an authentication system according to a second embodiment will be described. The authentication system of the second embodiment is characterized in that when user authentication is requested from an application server providing electronic commerce transaction and other services, a session key encrypted with a public key is received from the application server and is decrypted using a private key to recover the session key; then, the thus recovered session key and the result of the comparison done in the authentication system of the first embodiment are encrypted with the private key and returned to the application server, thus achieving highly reliable user authentication at the application server.

[0046] Figure 3 is a block diagram showing, in simplified form, the configuration of the authentication system according to the second embodiment. In Figure 3, the same constituent elements as those in Figure 1 are designated by the same reference numerals, and a description thereof will be omitted here. The authentication system shown in Figure 3 differs from that of Figure 1 in that not only the encryption key e1 but also information of a private key Es1 is stored in the personal information storage medium 30 to be loaded into the registering terminal 20 and the authenticating terminal 40, and in that the system includes an application server 50.

[0047] The application server 50 here is connected to the communication line 9 and provides various services such as electronic commerce transactions; further, the application server 50 acquires a public key to be paired with the private key Es1, and issues a session key Ks1 to the authenticating terminal 40 as part of a user authentication procedure. This

server is a computer system similar in configuration to the authentication information storing server 10.

[0048] The operation of the authentication system according to the second embodiment will be described below. Figure 4 is a flowchart illustrating the operation of the authentication system according to the second embodiment. In the operation of the authentication system according to the second embodiment, steps S101 to S103, S201, S202, and S301 to S304 are the same as the corresponding steps shown in Figure 2, and a description of these steps will not be repeated here. Among them, steps S101 to S103 and S201 shown in Figure 2 are not shown in Figure 4 to simplify the explanation.

[0049] Accordingly, the operation that follows the comparison (step S304) done in the authenticating terminal 40 will be described here. Suppose that after the comparison is done in the authenticating terminal 40, the user accesses the application server 50 with a desire to receive services provided by the application server 50; in this case, the application server 50 first generates a session key for that access by using random numbers. Next, the application server 50 encrypts the generated session key by using the public key Ep1 acquired in advance (step S401), and transmits the session key to the authenticating terminal 40 (step S402). The public key Ep1 acquired in advance by the application server 50 is a key specific to the user desiring to use the services provided by the application server 50, and is to be paired with the private key Es1 that the user holds.

[0050] The acquisition of the public key Ep1 by the application server 50 is accomplished, for example, by the application server 50 giving an instruction to the effect that the public key Ep1 is transmitted to the user when the user has accessed the application server 50 for the first time. The user may acquire the pair of keys, i.e., the public key Ep1 and the private key Es1 specific to the user, from a certification authority which is a trusted third party

body, or may acquire them by having the authentication information storing server 10 issue them; that is, the method of acquisition is not specifically limited.

[0051] When the encrypted session key is received from the application server 50, the authenticating terminal 40 decrypts the session key by using the private key Es1 recorded in the personal information storage medium 30 (step S305). Further, the authenticating terminal 40, using the private key Es1, encrypts the message indicating the result of the comparison done in step S304 and the session key decrypted in step S305 (step S306), and transmits them to the application server 50 (step S307).

[0052] When the encrypted comparison result and session key are received from the authenticating terminal 40, the application server 50 decrypts them by using the public key Ep1, and checks whether the decrypted comparison result indicates a match and whether the decrypted session key matches the session key transmitted to the authenticating terminal 40 in step S402 (step S403). If they match, it is determined that the access is from a legitimate user, and the application server 50 provides services by means of cryptographic communication combining the so-called common key cryptography and public key cryptography, using the above session key or a newly generated session key and the private key/public key pair.

[0053] In this way, when providing services to the authenticating terminal 40, the application server 50 usually issues a session key to enhance the security; in this embodiment, the session key is utilized for user authentication.

[0054] As described above, according to the authentication system of the second embodiment, in addition to the authentication system configuration of the first embodiment, information of the private key Es1 is recorded in the personal information storage medium 30, and the session key issued by the application server 50 and the result of the

biometric information comparison done in the authenticating terminal 40 are transferred using public key cryptography, thereby accomplishing the user authentication requested by the application server 50; accordingly, in addition to the effect of the first embodiment, the second embodiment can achieve highly reliable user authentication when seen from the application server 50.

[0055] Embodiment 3. Next, an authentication system according to a third embodiment will be described. The authentication system of the third embodiment is characterized in that a plurality of authentication information storing servers, each identical to the one shown in the first embodiment, are installed, and in that the authentication information storing servers each include a personal authentication information database whose contents are the same between the different servers.

[0056] Figure 5 is a block diagram showing, in simplified form, the configuration of the authentication system according to the third embodiment. In Figure 5, the same constituent elements as those in Figure 1 are designated by the same reference numerals, and a description thereof will be omitted here. The authentication system shown in Figure 5 differs from that of Figure 1 in that the system includes a plurality of authentication information storing servers 10-1 to 10-n.

[0057] In particular, the personal authentication information database 12 provided in each authentication information storing server stores the same contents, so that the registering terminal 20 and the authenticating terminal 40 can perform processing for registration or biometric information acquisition with any authentication information storing server.

[0058] For example, when the registering terminal 20 has registered biometric information with the authentication information storing server 10-1 as described in the first embodiment, the authentication information storing server 10-

1 reports any changes associated with the registration to the other authentication information storing servers 10-2 to 10-n, which then update the contents of their personal authentication information databases 12 accordingly.

[0059] That is, the authentication information storing servers 10-1 to 10-n are in the relationship of mirror servers relative to each other, and always hold the biometric information as identical contents. Accordingly, the authentication terminal 40 can acquire the latest biometric information from any of the authentication information storing servers. Here, the authentication information storing server located at the shortest distance in terms of the communication route length may be preregistered in the authenticating terminal 40 so that the preregistered authentication information storing server may usually be used. Here, provisions can be made to automatically to switch to another authentication information storing server when the preregistered authentication information storing server fails due to some trouble.

[0060] As described above, according to the authentication system of the third embodiment, since the biometric information is duplicated across the plurality of authentication information storing servers 10-1 to 10-n, if any one of the servers has failed the information can be retrieved from another server and decrypted, and reliable authentication can thus be ensured. Further, if the authentication information storing server having fast response speed is preregistered as the server to be used usually, quick authentication can be achieved irrespective of the network traffic condition, and even when the terminal that issued an authentication request and the registering terminal are located at geographically separated sites, the authentication can be done without being affected by the geographic separation.

[0061] Embodiment 4. Next, an authentication system according to a fourth embodiment will be described. The

authentication system of the fourth embodiment is characterized in that the biometric information input on the registering terminal is divided into a plurality of pieces of information which, after each piece of information is encrypted, are distributed across a plurality of authentication information storing servers for storage, and in that the encryption/decryption key information, registering terminal type information, user ID information, and information about the authentication information storing servers across which the biometric information has been distributed for storage are recorded in a transportable personal information storage medium.

[0062] Figure 6 is a block diagram, showing in simplified form, the configuration of the authentication system according to the fourth embodiment. In Figure 6, the authentication system according to the fourth embodiment comprises first to nth authentication information storing servers 100(1) to 100(n), a registering terminal 120, and an authenticating terminal 140, which are connected via a communication line 9 so as to be able to communicate with each other.

[0063] The first to nth authentication information storing servers 100(1) to 100(n) are each similar in configuration to the authentication information storing server 10 described in the first embodiment. However, the first to nth authentication information storing servers 100(1) to 100(n) here respectively hold different pieces of biometric information.

[0064] The registering terminal 120 is similar in configuration to the registering terminal 20 described in the first embodiment in that it comprises a personal authentication information input section 122 plus the personal information storage medium 30, but differs by the inclusion of an authentication information dividing section 124. The authentication information dividing section 124 is a means for dividing the biometric information, input via the

personal authentication information input section 122, into a plurality of pieces of information. For example, when a fingerprint image is captured by the personal authentication information input section 122, feature points based on feature point matching are extracted from the fingerprint image, and the extracted feature point information is divided into a plurality of pieces of information according to their kinds such as an end point or a branching point, their positions, and the spacing between ridges.

[0065] The authenticating terminal 140 is similar in configuration to the authenticating terminal 40 described in the first embodiment in that it comprises a personal authentication information input section 142 plus the personal information storage medium 30, but differs by the inclusion of an authentication information merging section 144. The authentication information merging section 144 is a means for reconstructing the original biometric information by merging together the biometric information divided by the authentication information dividing section 124.

[0066] The personal information storage medium 30 is, as in the first embodiment, a nonvolatile storage medium that is easy to carry, and the communication line 9 is no different from that shown in the first embodiment.

[0067] The operation of the authentication system according to the fourth embodiment will be described below. Figure 7 is a flowchart illustrating the operation of the authentication system according to the fourth embodiment. In Figure 7, as in the first embodiment, the user first inputs via the personal authentication information input section 122 of the registering terminal 120 the user's own biometric information that can be input on the personal authentication information input section 122 (step S111).

[0068] Next, the biometric information acquired by the registering terminal 120 is divided by the authentication information dividing section 124 into a predetermined plurality of pieces of biometric information (step S112). In

particular, the information is divided in such a manner as to correspond with the types of information to be stored in the first to nth authentication information storing servers 100(1) to 100(n), respectively.

[0069] Further, the registering terminal 120 applies encryption to each piece of biometric information by using a prescribed encryption key e1 (step S113). This encryption key e1 is recorded in the personal information storage medium 30 together with the user ID information, the type information of the registering terminal 120, etc. The encryption key e1 used here to encrypt the divided biometric information may be common to each piece of information or may be different for each piece of information. This encryption key e1 is recorded in the personal information storage medium 30 together with the user ID information, the type information of the registering terminal 120, and the server information of the first to nth authentication information storing servers 100(1) to 100(n) where the biometric information is registered.

[0070] Next, based on the server information recorded in the personal information storage medium 30, the registering terminal 120 transmits the encrypted pieces of biometric information via the communication line 9 to the first to nth authentication information storing servers 100(1) to 100(n) together with the user ID information, the type information of the registering terminal 120, etc. (step S114). Upon receiving the registration information including the encrypted biometric information, each of the first to nth authentication information storing servers 100(1) to 100(n) registers the registration information in its personal authentication information database 12 (step S211).

[0071] When the registration of the biometric information is completed in the above procedure, the user removes the personal information storage medium 30 from the registering terminal 120, and keeps it in a safe and secure manner, for example, by carrying it with him, as described in the first

embodiment, until it becomes necessary for authentication on the authenticating terminal 140.

[0072] Next, when using the authenticating terminal 140, the user loads the personal information storage medium 30 into the authenticating terminal 140. Then, for the user authentication that the authenticating terminal 140 requests when the user uses the authenticating terminal 140 by itself or to receive services provided via the communication line 9, the user inputs his biometric information via the personal authentication information input section 142 of the authenticating terminal 140 in the same manner as when inputting the biometric information using the registering terminal 120 (step S311).

[0073] The authenticating terminal 140 temporarily stores the biometric information input by the user, and transmits, together with the user ID information, the type information of the registering terminal 120, etc. recorded in the personal information storage medium 30, a request to each of the first to nth authentication information storing servers 100(1) to 100(n) determined by the server information recorded in the personal information storage medium 30 for transmission of the registered personal authentication information, that is, the encrypted biometric information (step S312).

[0074] Upon receiving the personal authentication information request from the authenticating terminal 140, each of the first to nth authentication information storing servers 100(1) to 100(n) retrieves from its personal authentication information database 12 the encrypted biometric information that matches the user ID information, the type information of the registering terminal 120, etc. contained in the personal authentication information request, and transmits the biometric information to the authenticating terminal 140 (step S212).

[0075] When the encrypted biometric information is received from each of the first to nth authentication information

storing servers 100(1) to 100(n), the authenticating terminal 140 decrypts the encrypted biometric information by using the encryption key e1 recorded in the personal information storage medium 30 (step S313). Further, in the authenticating terminal 140, the authentication information merging section 144 reconstructs the original biometric information by merging together the plurality of pieces of biometric information thus decrypted (step S314).

[0076] Then, the authenticating terminal 140 compares the thus reconstructed biometric information with the biometric information input in step S311, and determines whether they match or not (step S315).

[0077] When it is determined that they match, the authenticating terminal 140 makes a transition to a state in which the authenticating terminal 140 can be used by itself or used to receive services via the communication line 9, and displays a message or the like to that effect. Conversely, when they do not match, a message or warning or the like prompting the user to reenter biometric information is displayed.

[0078] As described above, according to the authentication system of the fourth embodiment, not only can the effect achieved by the first embodiment be obtained, but as the registration information is registered by distributing it across a plurality of authentication information storing servers, and the distributed pieces of information are retrieved from the servers and merged together at the time of authentication, the embodiment can also offer the effect of being able to avoid centrally managing the biometric information at a single server. Further, as each authentication information storing server only holds a fragment of the biometric information, user authentication cannot be done by using only the biometric information stored in one authentication information storing server; this ensures high security.

[0079] Moreover, as the personal information storage medium

30 which is carried from one terminal to another need only hold at least the server information designating the authentication information storing servers across which the biometric information is distributed and the types of the distributed pieces of biometric information, no strain is put on the capacity of the personal information storage medium 30 even if the size of the biometric information is large.

[0080] Embodiment 5. Next, an authentication system according to a fifth embodiment will be described. The authentication system of the fifth embodiment is characterized in that a plurality of authentication information storing servers, each identical to the one shown in the second embodiment, are installed as shown in the third embodiment, and in that the authentication information storing servers each include a personal authentication information database whose contents are the same between the different servers.

[0081] Figure 8 is a block diagram showing, in simplified form, the configuration of the authentication system according to the fifth embodiment. In Figure 8, the same constituent elements as those in Figure 3 are designated by the same reference numerals, and a description thereof will be omitted here. The authentication system shown in Figure 8 differs from that of Figure 3 in that the system includes a plurality of authentication information storing servers 10-1 to 10-n, as in the system shown in Figure 5.

[0082] As described above, according to the authentication system of the fifth embodiment, not only can the effect achieved by the second embodiment be obtained, but since the biometric information is duplicated across the plurality of authentication information storing servers 10-1 to 10-n, the embodiment can also offer the effect of achieving reliable authentication, because if any one of the servers has failed, the information can be retrieved from another server and decrypted. Further, if the authentication information storing server having fast response speed is preregistered as

the server to be used usually, quick authentication can be achieved irrespective of the network traffic condition, and even when the terminal that issued an authentication request and the registering terminal are located at geographically separated sites, the authentication can be done without being affected by the geographic separation.

[0083] Embodiment 6. Next, an authentication system according to a sixth embodiment will be described. The authentication system of the sixth embodiment is characterized in that each of the first to nth authentication information storing servers shown in the fourth embodiment is configured as an array of plurality of servers as shown in the third embodiment.

[0084] Figure 9 is a block diagram showing, in simplified form, the configuration of the authentication system according to the sixth embodiment. In Figure 9, the same constituent elements as those in Figures 5 and 6 are designated by the same reference numerals, and a description thereof will be omitted here. The authentication system shown in Figure 9 differs from that of Figure 6 in that a plurality of mirror servers are provided for each of the first to mth authentication information storing servers 10-1(1) to 10-1(m). For example, a plurality of first authentication information storing servers 10-2(1) to 10-n(1), in which the same biometric information is stored, are provided for the first authentication information storing server 10-1(1).

[0085] As described above, according to the authentication system of the sixth embodiment, a plurality of mirror servers are provided as shown in the third embodiment for each of the first to mth authentication information storing servers 10-1(1) to 10-1(m) across which the divided biometric information is distributed as in the authentication system of the fourth embodiment; accordingly, not only the effect achieved by the fourth embodiment, but also the effect achieved by the third embodiment can be obtained.

[0086] It will be appreciated that the configuration in which the divided biometric information is distributed across the plurality of authentication information storing servers each of which is provided with a plurality of mirror servers, as shown in the sixth embodiment, can also be applied to the authentication system of the second embodiment.

[0087]

[Advantageous Effect of the Invention] As described above, according to the present invention, the preregistered biometric information is managed by the externally located authentication information storing server; accordingly, even when the user desires to use a terminal, for example, the authenticating terminal, that is different from the registering terminal that the user used at the time of registration, personal authentication involving encryption can be done by just moving the personal information storage medium from one terminal to the other, while on the other hand, user authentication cannot be done on a terminal not loaded with the personal information storage medium; this offers the effect of ensuring high security.

[0088] According to another aspect of the invention, encryption key and private key information is recorded in the personal information storage medium, and the session key issued by the application server and the result of the biometric information comparison done in the authenticating terminal are transferred using public key cryptography; this offers the effect of being able to accomplish with high reliability the user authentication requested by the application server.

[0089] According to another aspect of the invention, as the registration information is registered by distributing it across a plurality of authentication information storing servers, and the distributed pieces of information are retrieved from the servers and merged together at the time of authentication, it becomes possible to avoid centrally managing the biometric information at a single server, and as

a result, user authentication cannot be done by using only the biometric information stored in one authentication information storing server; this offers the effect of ensuring high security.

[0090] According to another aspect of the invention, as the registration information is registered by distributing it across a plurality of authentication information storing servers, and the distributed pieces of information are retrieved from the servers and merged together at the time of authentication, and as encryption key and private key information is recorded in the personal information storage medium, and the session key issued by the application server and the result of the biometric information comparison done in the authenticating terminal are transferred using public key cryptography, not only does it become possible to avoid centrally managing the biometric information at a single server, ensuring high security, but there is also offered the effect of being able to accomplish with high reliability the user authentication requested by the application server.

[0091] According to another aspect of the invention, as the biometric information is duplicated across the plurality of authentication information storing servers, if any one of the servers has failed the information can be retrieved from another server and decrypted, thus offering the effect of achieving reliable authentication.